Are contracts concluded on the Internet valid and enforceable ?
An analysis of the Law applicable to contracting on the Internet

Faculty of Law, University of Cape Town

Supervisor: Associate Professor Julien Hofman,

A dissertation presented to the Faculty of Law, University of Cape Town, in partial fulfilment of the requirements of the degree of Master of Laws in approved courses and a minor dissertation. The other part of the requirement for this degree was the completion of a programme of courses.

Declaration

I declare that this dissertation is my own, unaided work. It is being submitted for the degree of Master of Laws at the University of Cape Town, South Africa. It has not been submitted before any degree or examination to any other University not has it been prepared under the aegis or with the assistance of any other body or organisation or person outside the University of Cape Town.

Cape Town, 15 April 1999

Craig Archbold

Acknowledgements

I would like to express my gratitude to Linda Krawitz of the Law library at the University of Cape Town for her assistance in locating source material for this dissertation.

I would like to thank Professor G Dolazalek for introducing me to the relationship between Law and computers.

Contents

Part One

Chapter One

1.1 Introduction

The Internet allows contractual negotiations to take place electronically between parties in different national and international jurisdictions. A commercial transaction may be concluded and performed electronically without the parties ever having met or communicated with each other in a formal or informal manner. [1]

It is a unique technology that may resemble an instantaneous telex in certain instances, and therefore, may invoke *prima facie* comparisons to the legal principles relating to telephonic or telex communication. However, in other instances the medium resembles a conventional post box, an analogy that immediately invokes the expedition theory. [2]

Commercial activity between consenting parties assumes its own course. The availability of graphic user interface browsers such as Microsoft Internet Explorer and Netscape has encouraged the mass adoption of the Internet by businesses and by private individuals. The absence of legislation or decided cases concerning the validity and enforceability of contracts has not prevented the formation and performance of commercial transactions using the medium of the Internet.

In 1955, before the development of the Internet, questions were already being posed concerning the rules relating to offer and acceptance and how they were affected by the then emergent technologies of the telephone and the telegram, before the advent of the telex. Our system of legal precedence was criticised for its inability to react to changes in technological innovation. In that time in our history it was acknowledged that South African law lacked

> "[A]uthoritative rulings on vital legal issues in fields of law which are the everyday meeting ground of disputing parties." [3]

At that time in the development of South African Law, parties who expected "the issue to assume concrete form in the shape of actual litigation," were cautioned not to expect guidance from our courts, as "...seemingly important and disputed points of law never reach this stage:"[4] Faced with uncertainty, risk averse parties tend to avoid litigation rather than

---

[1] <http://mbendi.co.za/werksmns/index.htm>
[2] The applicable South African case law is discussed below in Chapter Four
[3] Professor Ellison Kahn 1955 SALJ 246."Some Mysteries of Offer and Acceptance" at pg. 246
[4] idem n3

become involved in commercial disputes concerning undecided issues. While such disputes have the potential to clarify the legal position, they expose the parties to the possibility of a costly adverse ruling. The result of this reluctance is that the law lags behind technical innovation.

The frequency of disputes involving the validity and enforceability of Internet contracts has not reached the level where our courts have been called upon to clarify the legal position. Although the absence of traditional, face to face meetings between contracting parties and the lack of provisions dealing with the electronic equivalents to signatures to contractual documentation create uncertainty, our law has not reached the point where the disputes relating to Internet contracts are before the courts.

1.2 Scope of Analysis of this dissertation

1.2.1 International Contracts

An Internet contract may be international in nature where it is concluded between a South African party and a party whose principal place of business or registered office is in another jurisdiction.

1.2.2 Domestic Contracts

An Internet contract may be domestic in nature where it is concluded between parties who both have their principal places of business or registered office in the Republic of South Africa.

This dissertation deals with the relevant Law that a South African court would consider in hearing a domestic dispute as well as international legislation that an interested South African commercial party should be aware in dealing with another party in a foreign jurisdiction.

1.2.3 A Practical Guide

This dissertation attempts to adopt a practical approach to the issues concerning an Internet contract with a view to clarifying potential areas of dispute relevant to interested commercial parties.

1.2.4 References to Gender

All references to the male gender in this dissertation are solely for the purposes of clear analysis and are intended to apply equally and without bias to the female gender.

1.3 Relevant Legal Issues

In order to establish whether or not contracts concluded via the Internet are valid and enforceable, it is submitted that the following related sub-issues should be addressed:

1.3.1 Validity

1.3.1.1 Can a contract be formed by the actions of parties who communicate via the Internet?

1.3.1.2 Do these actions amount to sufficient consensus *ad idem* for the law to give effect to their actions?

1.3.1.3 Can the line of decided cases relating to the formation of contracts, setting out general principles of the law of contract, be of assistance to interested parties?

1.3.2 Enforceability

What would be the likely approach of a South African Court to a contractual dispute in terms of the current provisions relating to civil procedure?

1.3.3 Reference to Existing Foreign Legislation

1.3.3.1 If the line of decided cases do not provide assistance, should the issue be left to the courts to decide as and when a contractual dispute is brought before them by litigating parties? Or should legislation be tabled to remedy the apparent uncertainty posed by the uniqueness of the Internet?

1.3.3.2 If legislation would remedy uncertainty, what form should such legislation assume?

1.3.3.3 Can South African Law draw from the experience of other jurisdictions?

1.4 Structure

This dissertation consists of five parts each dealing with a different theme.

1.4.1 Part One deals with the background to contracting over the Internet.

1.4.2 Part Two deals with authoritative South African decided cases and the application of those cases to an Internet contract.

1.4.2.1 Chapter Four, dealing with the validity of an Internet contract looks at a line of decided cases arranged according to existing modes of communication.

1.4.2.2 Chapter Five, in respect of the enforceability of an Internet contract, relates more to decided cases on evidential issues.

1.4.3 Part Three of this dissertation deals with international legislation on general principles of electronic commerce.

1.4.4 Part Four of this dissertation deals with legislation relating specifically to digital signatures and certificate authorities.

1.4.5 Part Five of this dissertation relates to the findings of the analyses that have been conducted as well as appropriate recommendations.

In order to appreciate these issues an understanding of the background to and technology underlying the Internet is required.

Part One

Chapter Two - The Background to and Technology underlying the Internet

2.1 Background

2.1.1 What is the Internet?

L J Davies has compared a description of the Internet to a discussion between blind men as to what an elephant actually is.[5] Each participant or user of the Internet only senses one of several different aspects thereof and so comes up with his definitive description. He contends that the word Internet is thus probably best used as a descriptive noun, to cover the internetworking of networks.

2.1.2 History of the Internet

In the mid to late 1960's, the Department of Defence of the United States Government accepted the impact computers would have on education, research and development, and set up the Advanced Research Projects Agency (ARPA) to experiment with computer link-ups via telephone lines. The aim was to test whether a new technology called "packet switching" could be used to send information to linked computers. The project was initially aimed at the formation of a data network that could survive a nuclear attack, so that if one part was destroyed, communication was still possible. Later, it became a tool for national research and development projects.

The growth of the network allowed researchers to exchange information and electronic mail. The latter was revolutionary, allowing letters to be sent at the speed of a telephone call. In the 1970's, ARPA helped develop rules and protocols for transferring data reliably and simply between different computer networks. The availability of these protocols encouraged the exponential expansion of their application to colleges, research companies and agencies connected to the network. Companies began offering private individuals links to the network. Person to person communication quickly exceeded the use of the network as a tool of long distance computing. What had started as a government experiment, had become a private enterprise.

2.2 Packet switching

The Internet is dependent on a technology known as packet switching. Packet switching is a method of sending data between networks where no known path is set up in advance. This concept is easiest to understand when compared to circuit switching, employed when dialling

[5] <http://www.ccls.edu/itlaw/publications/html/inetiba.html;>; The Internet and the Elephant

a telephone. Once a valid telephone number is dialled, a traceable circuit between both the initiating and receiving instrument is established. This circuit is solely dedicated to that call.

Packet switched networks use an entirely different technique. Each document, image, sound, or any other type of file that needs to be sent over the Internet is first broken down into a set of approximately equal sized chunks called packets. A packet usually holds 128 bytes of data. Each byte consists of a string of eight binary digits or bits representing a zero or a one. Each packet contains approximately 1024 bits of data and consists of the following segments or frames of identifying information:

2.2.1 A 16 Bit Start Frame;

2..2.2 A 64 Bit Header;

2.2.3 A portion of the data being sent (approximately 113 bytes or 904 bits);

2.2.4 A 16 Bit End Frame;

2.2.5 A 24 Bit Error Control Frame.

A six page ASCII (American Standard Code for Information Interchange) text document file of approximately 12 Kilobytes or 12 000 bytes or 96 000 bits in size would be broken into approximately 107 packets. The 64 Bit header contains a string of information referred to as the message number, destination, source, link number and packet number. This makes each packet unique. [6]

Data packets are transmitted, along with the unique addresses of the sender and receiver of the packet. Packets are sent out of the sending computer to a local network or service provider. They are then picked up by a router whose function is to ensure that packets are forwarded along to other networks until they eventually arrive at their intended destination. Routers are computers that are dedicated to "reading" header information and determining which router to send the packet to next. In this respect, packets are very similar to mail in a postal system, only much faster.

2.3 Transmission Control Protocol/Internet Protocol

The communications technology that allows networks to connect with each other is a suite of protocols referred to as TCP/IP. This term, which stands for 'Transmission Control Protocol/Internet Protocol', is misleading as the protocol suite consists of a large set of

[6] Management Information Systems 4th edition, K C Laudon & JC Laudon, Prentice Hall 1996 Pg. 322

protocols, of which the transmission control protocol (TCP) and internet protocol (IP) are but two of several. The suite consists of layers of protocols.

TCP/IP works by providing functions to break up a piece of digital data into small packets or datagrams and then transports those packets across any combination of networks to their destination. Neither the actual route nor the communications hardware that constitute that route matter.

2.3.1 Network Interface Layer

Network Interface Layer is at the base of the model and is responsible for managing frames in conjunction with the Wide Area Network (WAN) or Local Area Network (LAN) Technologies that may underlie a network . IP uses Network Driver Interface Specification (NDIS) to submit frames to the network interface layer. Ethernet, Token Ring, and ArcNet are examples of LAN Technologies supported by IP. WAN Technologies are generally divided into serial line and packet switched networks, both of which are supported by IP. Packet switched networks include X25, Frame Relay and ATM (asynchronous transfer mode). Serial lines include, dial up analogue, digital lines and ISDN lines.[7]

2.3.2 The Protocol Stack

This layering of protocols is called a protocol stack. The idea behind this model is that each layer provides its own set of functions to the stack, and uses the functions provided by the layers below it. The structure is flexible enough to allow each layer to be updated independently, added-to, and developed without affecting the integrity of the layers below or above it.

2.3.3 Internet Protocol Layer

The next layer up is the lowest level of protocol, the Internet protocol layer. It merely provides the basic transport layer and addressing facilities. The most common protocol used is the Internet Protocol or IP. This protocol provides a connectionless service with no error correction facilities, a best efforts protocol. It neither knows nor cares whether the data packets arrive at their destination. The addressing works by using a unique 32-bit binary number, the IP address, for each interface to the protocol stack. A single computer can have more than one interface and so more than one IP address. These numbers are often expressed as a series of four octets for convenience, e.g. 140.142.4.238.

---

[7] Internetworking with Microsoft TCP/IP in Microsoft Windows NT 4.0, Microsoft Corporation 1997 Pg. 41

Internet protocols encapsulate packets into Internet datagrams and run necessary routing algorithms. There are four Internet protocols.

2.3.3.1 Internet Protocol is primarily responsible for addressing and routing packets between hosts and networks.

2.3.3.2 Address Resolution Protocol is used to obtain hardware addresses of hosts located on the same physical network.

2.3.3.3 Internet Control Message Protocol sends messages and reports errors regarding the delivery of a packet.

2.3.3.4 Internet Group Management Protocol is used by IP hosts to report host group memberships to local multicast routers.[8]

2.3.4 Transport Layer Protocols

The next layer of protocols, the transport layer protocols, provide the link between the application layer protocols and the Internet layer protocols. Two of the most common are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

2.3.4.1 TCP provides a connection-based service that includes error correction to provide a reliable link between two computers. To provide reliability, however, TCP incurs a large overhead in terms of processing required, and information stored in the individual datagrams. Thus, more datagrams are required with TCP than with UDP.

2.3.4.2 UDP provides a basic connectionless service without any error correction facilities. It has a low processing overhead and requires only a small amount of information to be stored in the datagrams that it transmits. It can be used to broadcast as it can transmit to a single interface or multiple interfaces without difficulty.

The transport layer protocols provide an address called a port, a 16-bit number, for the applications layer protocols to use. Each service provided by the applications layer uses one or more unique ports when transmitting or receiving information. Certain services such as Telnet, or hypertext transfer protocol (HTTP) have had port addresses specified as defaults.

---

[8] idem supra n 7 at pg.38

Others such as file transfer protocol (FTP) will use both default ports and extra ports that are dynamically allocated to the service as and when they are needed. To create a full numerical TCP/IP address the port address is appended to the end of the IP address

A second form of addressing, the domain name system (DNS), which uses a set of more user-friendly symbols, can be added to the basic addressing. The DNS is hierarchical in structure and works by using a set of named domains. A unique address can thus be constructed. As the DNS is independent in structure from the IP addressing system, domains can be chosen for the convenience of the users or network administrator. An example of such an address is the address of the Internet Law & Policy Forum, http:// www.ilpf.org.

2.3.5 Applications Layer

At the top of the stack model is the Applications layer, where the network allows applications such as POP, FTP, Telnet, SMTP and DNS to gain access to the network. SMTP stands for Simple Mail Transfer Protocol and is used to send electronic mail. POP stands for Post Office Protocol and is used to receive electronic mail from a server at a remote location. A specific electronic mail software programme or application may offer an end user the option of using one protocol to send and another protocol to receive electronic mail. For example SMTP may be used to send for outgoing mail from a remote PC to a network node and POP may be used to receive mail from a dedicated electronic mail server at that network node.

2.4 Domain Name Systems

The Internet requires each computer connected to it, usually called a host, to have a unique address. When connecting to a Web site, one of the first things that happens is the computer attempts to make a connection to the DNS to find out what the IP address is for that site. Once the DNS translates this hostname and sends back the IP address, it becomes the destination address for packets going out to that site. In order to accomplish this translation, various computers around the Internet are designated as domain name servers and answer requests for IP addresses for particular hostnames.

A more accurate name for the domain name is the Fully Qualified Domain Name (FQDN). One can always use the actual IP address in place of the domain name, for example: http://140.142.4.238 will access Internet Law & Policy Forum's home page in the same fashion as http:// www.ilpf.org.

2.5 Universal Resource Locator

This line indicates the exact location of the resource that the browser has loaded at that time in URL format. URL stands for Universal Resource Locator. It is the standard for specifying resources accessed over the Internet. It provides four main types of information.

2.5.1 Method - The tool (http, gopher) needed to access the information.
2.5.2 Hostname - The Internet address of the computer that has the resource.
2.5.3 Filename - The name of the file that has the resource.
2.5.4 Path - The location of the file in the directory structure at the hostname.

For example < http://140.142.4.238/digsig/survey.html>[9]

2.6 How E-Mail Is Transmitted

When an e-mail message is sent across a network the following occurs: Data that makes up an e-mail message is split into packets by the IP portion of TCP/IP. IP also adds header information to each packet. Using header information in the packets, routers determine the best path for each packet to take to its final destination. The TCP portion of TCP/IP reassembles the packets in the correct order and ensures that all packets have arrived undamaged.

Packets move from router to router until they reach their final destination, in much the same way that an envelope travels between postal substations before reaching the recipient. The packets that make up data, such as an e-mail message or a web page, will not necessarily all follow the same route to the final destination. The route that a packet travels depends on many variables, including network traffic at that particular moment and the size of the packet being sent.[10]

---

[9] This is the address of a document published by the Forum that is referred to in this dissertation; Survey of Electronic and Digital Signature Legislative Initiatives in the United States

[10] <http://www.phdsystems.com/tutorials/internet/ipadress/sld05.html>

Part One

Chapter Three - How Parties Contract Via The Internet?

3.1 The Place Where the Contract is concluded

3.1.1 Principal Place of Business

Depending on the technological sophistication of the parties, the place of transmission and receipt may be at the parties' principal place of business. This would occur when such parties have a dedicated connectivity link to the Internet controlled by a permanent gateway server that forms part of the parties' LAN.

3.1.2. The Network Node of A Professional Intermediary

Alternatively one or both of the parties may make use of the services of a professional intermediary or Internet Service Provider (ISP) at a separate remote location which may or may not be in the same jurisdiction as their principal place of business. E-mail and the World Wide Web are both Internet "capabilities" which rely on client/server technology. Both e-mail messages and World Wide Web home pages must reside on a server connected directly to the Internet. [11]

3.1.2.1 E-mail "Post Office" Service

The ISP provides a network node or point of presence (POP) to such a party where e-mail that is sent to the party is received and stored on behalf of the party. In order to send or receive e-mail such a party must gain access to the network node from his place of business.

3.1.2.2 Place of Receipt and Transmittal of Packets

Similarly the ISP provides a point of access to a client at a remote location to access the World Wide Web through the network node of an ISP.

3.1.3 Multiple Network Nodes

A party may access more than one network node of the ISP if such a party has more than one principal place of business or by use of a readily transportable laptop computer. In such an instance an alternative or secondary place of receipt or transmission may or may not be at the principal place of business. This creates a range of alternatives, none of which can be held to be authoritative by reference to South African Law.

---

[11] idem supra n 2 at pg. 355

3.1.3.1 The network node closest to the main place of business may be deemed to be the place of receipt or transmission; or

3.1.3.2 The network node where the offeror's or offeree's transmission or receipt was in fact transmitted or received may be deemed to be the place of receipt or transmission and principal place of business; or

3.1.3.3 The network node usually used by the party for transmittal and receipt of messages may be deemed to be the place of receipt or transmission and principal place of business.

3.2 Access via Telkom SA Limited (Telkom)

3.2.1 Method of Access

This is usually done using a personal computer (PC) or workstation connected to a LAN, operating communication software and a modem or router connecting the PC or workstation to a Telkom service connection. The network node of the professional intermediary may also be accessed via one of the two South African commercial cellular service providers, MTN or Vodacom. However in most cases a party will access a POP by way of Telkom's telephone line or telecommunication service.

3.2.2 Telkom's Involvement

3.2.2.1 The South African Telecommunications Regulatory Authority (SATRA) derives its powers from s 5(2)(b) of the Telecommunications Act, 1996. Section 2 of the Act imposes a principal obligation on SATRA to regulate telecommunications services in the public interest.

3.2.2.2 SATRA distinguishes between Value Added Network Services (VANS) licenses and Public Switched Telephone Service (PSTS) licenses.

3.2.2.3 In terms of section 40 of the Act SATRA have granted a single PSTS license to Telkom in terms of which Telkom has a monopoly over PSTS.

3.2.2.4 This monopoly does not extend to VANS licences.

3.2.2.5 SATRA has held that Internet access provision falls under the definition of the VANS license.

3.2.2.6 However ISP's have to obtain a licence from Telkom to operate a VAN pursuant to Notice SRF-0001 (Notice 1811 of 1997) published in Government Gazette No. 18462. Section 2.1 of the regulation states that it "will suffice for an applicant to state that (s)he/it intends to conduct any or all of the services set

out in section 40 (2) of the Act and under the definition of the VANS in the Licence issued to Telkom SA Limited in terms of section 40 of the Act".

Where one or both of the parties use an ISP they usually access a network node of the ISP via Telkom's PSTS network or an Integrated Services Digital Network (ISDN) or a dedicated diginet connection.

3.3 Electronic mail ("e-mail")

This is the most popular and most widely adopted application of the Internet

3.3.1 Making an offer by e-mail

3.3.1.1 A party may send an e-mail to another party containing an offer sent with the intention that the recipient may accept the offer. The recipient may elect to accept the offer by way of an e-mail reply, or in person or by communicating his acceptance by way of a posted or personally hand-delivered letter, a telegram, a telex message or a telefax.

3.3.1.2 A party may transmit an e-mail to one or more other parties that may or may not amount to an operative offer made with the intention to contract.

3.3.1.3 Such a transmitted e-mail may amount to an invitation to do business or to an enquiry concerning the goods or services of another party.

3.3.1.4 Where the offeror has expressly stipulated that the offer may only be accepted by return of e-mail and by no other mode of communication, the recipient offeree is compelled to accept the offer via e-mail should he wish to contract.

3.3.2 Accepting an offer by e-mail

3.3.2.1 A party may send an e-mail accepting an verbal offer that has been made on a previous occasion in person or by telephone.

3.3.2.2 A party may send an e-mail accepting a written offer received by him on a previous occasion in the form of a posted or personally hand-delivered letter, a telegram, a telex message or a telefax.

3.3.2.3 A party may send an email accepting an offer received by him on a previous occasion in the form of an electronic e-mail file transmitted by the offeror via the Internet.

3.4 The World Wide Web

The World Wide Web is simply an information retrieval tool, which uses a set of commands known as HTTP (hypertext transport protocol). The World Wide Web allows retrieval, formatting and information display of text, audio, graphics and video using hypertext links and is often regarded as synonymous with, and used interchangeably with the term "Internet", due to the impact which it has had on the commercial use of the Internet.

3.4.1 Accepting an offer made on the World Wide Web by e-mail

A party may send an e-mail in reply to information which is set out to the world at large on a World Wide Web site consisting of one or more pages in an electronic form known as HTML (hypertext mark-up language) The person or organisation who is responsible or assumes responsibility for the website ("the website owner"), simply allows access to the web site through a home page.

Where the information is set out in the form of an unequivocal offer, a party may accept by responding by e-mail to the offer. If the web site contains terms and conditions of acceptance which are clearly accessible and identifiable, logic would dictate that they govern the contact but there are no decided cases on this point.

3.4.2 On-line acceptance without e-mail

Where the HTML format of the website has been designed to allow retrieval of input from the PC or a network workstation of a person who is accessing the web site, HTTP initiates a two way flow of datagrams between the server hosting the website and the client accessing the website from a PC or workstation. Where a website has been designed in such a manner, the client may initiate a transmission of datagrams to the host server responding to content provided on the host server.

This transmission will, in nearly all cases, be in response to a portion of the document contained on the web site which is "tagged" with HTML to link the client to other related pages which may or may not be on the same web database on the same server or on a separate server on the World Wide Web.

Such a related page may link to a page which sets out terms of acceptance and may provide for a HTML tag which allows the client to accept the offer as contained in the web page or collection of linked web pages.

Website owners set up websites to either make offers or to invite offers. Due to the unilateral mechanism by which information content tends to flow on the World Wide Web, the vast majority of websites amount to offers open to the world at large for anyone to accept while on line, using HTML datagram interchanges, or by providing an e-mail address where acceptance will be received.

In order to invoke favourable terms and conditions, website owners usually employ a "web-wrap agreement' where a client must click a link labelled "I agree" in order to initially access the website while on line. The client acknowledges acceptance of the terms and conditions of any future contract that may be concluded while on the website by the act of clicking such an "I agree" icon.[12]

The client may then during the same session and while still accessing the web site, purchase goods or services by clicking a similar "I accept" or "I agree" icon by which the client signifies his intention to accept the offer contained on the website on the terms and conditions set out by the website owner. These terms and conditions may be located on the same page as the icon itself or they may be on a separate page on the same site.

3.5 The Importance of Acceptance in Concluding the Contract

Acceptance appears to be the critical aspect of contracting via the Internet due to the nature of the implemented technology itself. It is therefore submitted that an enquiry into the decided cases in our law should focus primarily on the formation of the contract. Such an enquiry should target, in particular, how our law has dealt with offer and acceptance using analogous modes of communication.

[12] Paula Bagraim, "Contracting in Cyberspace" in Juta's Business Law 1998 Vol. 6 part 2. Pg. 54

Part Two

Chapter Four - The Validity of an Internet Contract - Decided Cases According To Modes of Communication

4.1 Contracts entered into through the Post

Professor Ellison Kahn set out four differing theories regarding contracts entered into through the post.[13]

4.1.1 The Declaration Theory

Acceptance takes place as soon as the offeree has expressly declared his assent by writing the reply, notwithstanding that no notice of the acceptance had been received by the offeror. It is enough that there is outward manifestation of acceptance and no need for the will to contract to be communicated to the offeror.

4.1.2. The Expedition Theory

Acceptance takes place when the letter of acceptance is posted.

4.1.3. The Reception Theory

Acceptance takes place when the letter of acceptance reaches the offeror's address before it comes to mind and before it reaches his mind.

4.1.4 The Information Theory

Acceptance only takes place when it reaches the mind of the offeror.

4.2 Decided Cases in South African Law dealing with Contracts entered into through the Post

4.2.1 In Cape Explosive Work Limited v S.A. Oil and Fat Industries Ltd 1921 CPD 244. at 265 to 266, Kotze J, held that the Post Office was the authorised means of communication with the consequence that a contract is concluded as soon as the letter of acceptance is posted.

4.2.2 In Kergeulan Sealing and Whaling v Commissioner for Inland Revenue 1939 AD 488 the Appellate Division quoted references to English, Scots and American law in confirming the operation of the expedition theory regarding contracts by post. Where the offeror

[13] 1955 SALJ 246."Some Mysteries of Offer and Acceptance" at pg. 254

authorises the offeree to make use of post to communicate his acceptance, the contract is concluded when and where the letter of acceptance is posted. For this rule to apply:

4.2.2.1 The contract must be in the nature of a commercial transaction;

4.2.2.2 The letter of acceptance must not have been incorrectly addressed;

4.2.2.3 The offeror must not have stipulated that he will not be bound until he receives or reads the letter of acceptance.[14]

4.2.3 Goldstone J commented on the Kergeulen case in SA Yster en Staal Industriele Korporasie Bpk v Koshade 1983 (4) SA 837 (T), where the court was concerned with the exercise of an option before a stipulated date by post. The court held that the expedition theory was subject to the overriding consideration of the intention of the parties either express or implicit and held *in casu* that it could be implied from the wording of the option that notification was only to be effective on reaching the offeror, not at the moment of posting,[15]

4.3 Contracts entered into by telegram

4.3.1 In Yates v Dalton 1938 EDL 177, the expedition theory was applied to contracts by telegram.

4.3.2 In Hirsch v Nel 1948 (3) S.A. 686 (A), a cessionary signed an acceptance on the option document itself and thereafter sent a telegram to the alleged cedent stating that the option had been ceded to him and that it was thereby accepted and exercised by him. The court held on these facts that communication of the acceptance by telegram was sufficient compliance with the then government legislation in the Orange Free State, i.e. Sec. 4 of Ord. 12 of 1906.

4.3.3 In Entores Ltd v Miles Far East Corporation (1955) 2All ER 493 the Court of Appeal refused to extend the expedition theory to telegrams. The question in issue was where a contract had been concluded, The Plaintiffs contended that it had been formed in England while the Defendants contended that the contract had been formed in Holland. The contract was formed by way of an interchange of telex messages between the Plaintiffs in London and the Dutch company in Amsterdam. It was held by the Court of Appeal that telex communications do not differ in principle from communications *inter praesentes* and that in

---

[14] Business Transaction Law, Robert Sharrock, 4th edition . Juta and Co. 1996 at pg. 49
[15] M C J Olmesdahl 1984 (101) SALJ " Unheralded Demise of Wolmer v Rees" at pg. 547

instantaneous communication there is no fact of expediency which requires a departure from the ordinary rule that acceptance must be notified. The contract was accordingly completed only when the message of acceptance was received on the Plaintiff's machine in London and therefore had been made in England.

Denning and Parker, LJJ stated explicitly that the same principles would apply in the case of a contract by telephone, namely that words of acceptance spoken into the telephone by the offeree are in effect to conclude the contract. If the line had gone dead or if the offereror did not hear the acceptance, a contract would not result.[16]

4.3.4 In Brinkibon Ltd v Stahag Stahl und Stahlwarenhandlsgesellschaft mbH [1983] (1) All ER 293 (HL) the Court was again called upon to establish where a contract entered into by telex had been concluded on similar facts to the Entores decision. A counter offer had been sent by telex by an Austrian company from Vienna to London on 3 May 1979 which had been accepted by an English company on 4 May 1979.

At 300H to 301B Lord Brandon stated;

> "The general principle of the Law applicable to the formation of a contract of offer and acceptance is that acceptance of the offer by the offeree must be notified to the offeror before a contract can be regarded as concluded. See Carlhill v Carbolic Smokeball Co. [1893]1QB 256 (at 262). The cases and acceptance by letter and telegram constitute an exception to the general principle of contract. The reason for the exception is commercial expediency.
>
> [T]hat reason of commercial expediency applies to cases where there is bound to be a substantial interval between the time when the acceptance is sent and the time when it is received. In such cases the exception to the general rule is more convenient and makes on the whole for greater fairness than the general rule itself would do. In my opinion however, that reason of commercial expediency does not have any application when the means of communication employed between offeror and offeree is instantaneous in nature as is the case when either the telephone or telex is used. In such cases, the general principle relating to the formation of contracts remains applicable with the result that the contract is made where and when the telex of acceptance is received by the offeror."

At 297C Lord Fraser stated;

> "An acceptance sent by telex directly from the acceptor's office to the offeror's office should be treated as if it were an instantaneous communication between the principles like a telephonic conversation. One reason is that the decision to that effect in Entores Ltd v Miles Far East Corporation (1955) (2) All ER 493 seems to have worked without leading to serious difficulty or complaint from the business community."

---

[16] C C Turpin Acceptance of Offer: "Instantaneous Commuication"1956 73 SALJ 77 at pg. 79

Lord Wilberforce at 296 C to D commented as follows:

> "Since 1955, the use of the telex communication has been greatly expanded and there are many variants on it. The senders and recipients may not be the principles to the contemplated contract. They may be servants or agents with limited authority. The message may not reach or be intended to reach the designated recipient immediately; messages may be sent out of office hours or at night, with the intention, or on the assumption that they will be read at a later time. There may be some error or default at the recipient's end which prevents receipt at the time contemplated and believed by the sender. The message may have been sent and/or received through machines operated by third persons. No universal rule can cover all such cases; they must be resolved by reference to the intentions of the party by sound business practice and in some cases by judgment where the risks lie."

4.3.5 In Westinghouse Brake & Equipment (Pty) Ltd v Bilger Engineering (Pty) Ltd 1986 (2) SA 555 (A) Fleming, J.A. analysed in some detail the issues revolving offer and acceptance in South African law. At 300 E the learned Judge commented on the case of Driftwood Properties (Pty) Ltd v McLean 1971 (3) S.A. 591 (A) as support for the contention that a starting point to the enquiry is that unless the contrary is established, a contract comes into being where the offeror gets to know of the acceptance of his offer. At 301G he held further that based on the Driftwood Properties decision, SA law on acceptance

> "[I]t must be taken that communication of acceptance is necessary for the conclusion of a contract unless a sufficient factual basis for reaching the conclusion that a contrary intention should prevail is established.

At 302B the learned Judge stated

> "[T]here is no authority as yet that the forced reasoning, which applies to results of offers, submitted by letter will apply to an offer submitted by telegram or telex. If the mere fact that an offer was submitted by post is such a forcible or irresistible factor in assessing the intention of the parties, it may well be that similar weight can become appropriate to the fact that agreement is to be concluded in writing or contains an execution clause or is concluded by businessmen in a commercial setting."

At 303G the learned Judge stated;

> "When a contract is concluded, including a commercial contract, the effect upon the parties according to whether the contract is concluded by mere acceptance or by communication thereof, may be a pointer of their intention and in an appropriate case a particularly cogent or even convincing consideration. In such a situation it is logic that prevails and not the mere fact that a commercial transaction is being concluded which binds logic."

4.3.6 In CGEEL Stone Equipment Enterprises Electronic South Africa Division v GKN Sankey (Pty) Ltd 1987 1 S.A. 81 (A) the Court held that the Respondents tender document and addendum thereto had been an offer which the Appellant had accepted by way of telex.

The Appellant had submitted that the telex did not result in the conclusion of a contract at that stage since there were a number of matters vital to the contract on which agreement had not been reached. At 87 D Corbett J.A., as he then was, commented on the dictum of Watermeyer, ACJ in Reid Brothers South Africa Limited v Fisher Bearings Co. Ltd 1943 AD 232 at 241 that a binding contract is as a rule constituted by the acceptance of an offer.

4.3.7 In Clipper Maritime Ltd v Shirlstar Container Transport Ltd (The Anemone) 1987 1 LLR 546 Staughton, J. in considering whether a telex might constitute a guarantee in writing and signed for the purpose of the Statute of Frauds, said obiter

> "I have reached the provisional conclusion in the course of the argument that the answer back of the sender of a telex would constitute a signature whilst that of the receiver would not since it only authenticates the document and does not convey approval of its contents."

The learned judge held at 557 that three separate telexes together with the possible addition of an actual charter party formed a sufficient memorandum of agreement.

4.3.8 In Shell Co of Australia Ltd v National Shipping Bagging Services Ltd [1988] 2 CA 1, telex communications between the parties were analysed in considering whether Shell could be imputed to being a party to a charter party, although it was found to not be party to the agreement.

4.4 Telephonic Contracts

4.4.1 In Wolmer v Rees 1935 TPD, 319 the parties negotiated over the telephone and the Court reasoned as follows:

4.4.1.1. The Rule that acceptance is complete upon posting is the consequence of an implied authorisation of the offeree to make use of the Post Office.

4.4.1.2. In the present case the offer was made over the telephone and the offeree was thereby authorised to use the telephone in accepting it.

4.4.1.3. Therefore, the acceptance was complete as soon as it was uttered into the telephone[17].

4.4.2 In Tel Peda Investigation Bureau (Pty) Ltd v Van Zyl 1965 4 S.A. 475 (E) Jenet J.P. was invited by Counsel for the Defendant to confirm the authority of Entores Limited in South

African law and to disagree with Woolmer v Rees 1935 TPD 319. The dispute before the court concerned a telephonic contract. The Court accepted the authority of the Entores decision and held that the contract was concluded only when and where the offeror heard the acceptance. The learned judge expressly disagreed with the reasoning in Woolmer's case and cited with approval the approach of Lord Denning's argument as being clear and convincing.

4.4.3 In S v Henkert 1981 (3) S.A. 445 (A) Rumpf, C J approved of the Tel Peda Investigation Bureau decision and confirmed the Court's disapproval of the Woolmer v Rees decision. The accused had been convicted in trading in Tiger's Eye in contravention of Act 77 of 1977. On appeal to the Provincial Division, the accused's conviction was set aside on the ground that delivery had taken place in South West Africa where the act did not apply. The State appealed on the ground that the agreement was in fact concluded in the Republic. Rumpf, C J stated at 541 that the accused had telephoned from South West Africa and had ordered a specific amount from the seller at a price already established. The Seller accepted the order and the accused heard the acceptance of the offer in South West Africa. The learned Chief Justice then held that the contract was concluded in South West Africa

The endorsement of the Tel Peda decision, based on the Entores case, in S v Henkert aligned South African law with English law and most continental systems..[18] The Entores decision is authoritative in Scotland (BM Walker, the Law of Contract in Scotland, para. 7.62) and in Australia (Telleman & Co. (Pty) Ltd v Nathans Merchandise (Victoria) (Pty) Ltd 1957, 98 CLR 93 at 112.)

4.4.4 In Lambons (Edms) Bpk v BMW (Suid Afrika) (Edms) Bpk 1997, 4 141 (A) the Court was called upon to decide whether a binding verbal agreement was concluded during a telephone conversation in which the Appellant averred that he had been appointed as a non-exclusive dealer in Bloemfontein by the Respondent. The issue was whether a legally enforceable contract had come into being. The Court arrived at the decision that there had been certain essential provisions regarding the rights and duties of the parties that had not been agreed upon which were not canvassed and accordingly a contract had not come into being. In principle the court accepted that a telephonic contract was binding, but, in casu, the

---

[17] idem supra n 16 at pg.77 for further commentary on this case
[18] idem supra n 15 at pg. 549

court accepted the Respondent's contention that detailed ancillary issues relating inter alia to profit arrangement had to be agreed upon before a binding contract was concluded.

4.5 Contracting via Telefax

There are no cases in South African or English law concerning the formation of a contact via the fax machine. However there are decided cases which deal with the approach of the courts to this relatively new technology.

4.5.1 In Cairn and another v De Bono 1 WLR 1988 at 1107 Sir Nicholas Brown Wilkinson V.C. held at 1112 that a faxed document amounted to a "completion statement" in writing. This statement was required in terms of a prior written contract between the parties for the sale of immovable property.

It was held further that the faxed document overrode a clause in the contractual agreement that stated;

> "12(H) any notice given to either party under the presence of this agreement shall be in writing and shall be deemed to have been served at the expiration of 48 hours after it has been posted."

The faxed document was admitted to prove earlier receipt of notification.

4.5.2 In Southern Witwatersrand Exploration Co. Ltd v Bishi Mining PLC and others 1998 (4) SA 767 (W), Cameron J was required to decide on the validity of a resolution of the Board of Directors waiving a condition precedent to a contract by means of a telefax which eventually consisted of 2 separate pieces of paper. The learned Judge held at 774 D that the actions of the directors yielded a resolution in writing signed by the directors in accordance with their articles of association and in accordance with the companies Act No. 61 of 1973 as amended.

In particular, at 778 A the learned Judge stated

> "...for when does the resolution signed by all directors come into existence? Even on face of a single composite resolution, the directors accumulated signatures actually exist only in electronically reproduced form. There is no single resolution bearing the original signatures of all the directors. Strictly therefore, the applicant's argument must entail that no resolution produced by fax will suffice. In the present case if De Villiers, instead of filing his signed copy had faxed to Stavrakis in Johannesburg for collation with Stavrakis already signed copy could it be said that a resolution in writing signed by all the directors does not exist.

> It does not seem to me so. To deny that it seems would be an exercise in undue formalism which may have stultifying effect upon commercial interaction. Facsimile transmissions constitute still relatively new technology. Other innovations including the world wide electronic internet [sic] may from time to time raise difficult questions of substantive compliance and proof. It would be in my view wrong to decide on them in an unduly formalistic basis. The question of proof is principally relevant to what substantive compliance with a specific procedure requires as it bears on the rationale of the procedure. In the present case, the rationale for article 76 is the avoidance of the requirement that a director's meeting be formally convened and held. That it does at the premium of a written signed unanimous resolution. It seems to me that there was such a resolution although it existed in two parts and in different locations. I therefore conclude there was compliance with article 76."

While this case does not deal with the formation of a contract by offer and acceptance, the obiter dictum of Cameron J provide authority for proposition that a telefax validly amounts to writing. It is therefore submitted that where parties exchange telefaxes containing offers or acceptances for the purposes of entering into a contract or where a party accepts the terms and conditions of a prior offer by way of telefax, the telefax itself may be admitted to prove that a contract was concluded.

4.6 Contracting via E-mail

There are no cases in South African law concerning the formation of a contact via the interchange of electronic mail. However, one decided case involves the approach of the courts to this relatively new technology.

In Council For Scientific And Industrial Research V Fijen 1996 (2) S.A.(A) concerning an action in terms of the Labour Relations Act 28 of 1956 for repudiation of an employment contract, the mode of repudiation of the employment contract per e-mail was regarded as a coherent part of a series of other forms of communication which included hand-written and typed documents. The Court accepted a printout of an e-mail made by the Respondent in which he made it clear that he wished only to remain in the Appellant's employment for as long as it took him to induce Appellant to sever relations with him on a basis which he found acceptable.

Part Two

Chapter Five - Enforceability of an Internet Contract

5.1 Is an Internet contract "written" or "signed" by the parties?

An Internet contract exists in electronic form. While it may be thereafter printed and thereby rendered onto paper, it is not signed nor does it even exist as a written document in a formal sense. In order to appraise the validity of a contract entered into via the Internet, it is submitted that our courts would in a hypothetical example, consider:

5.1.1 What constitutes "writing" in South African Law?

5.1.2 What constitutes a "signature" in South African Law?

5.2 Legislation Which Prescribes Written Form

A court may consider legislation which prescribes a contract or written instrument's format. The following non-exhaustive list of documents must be in written form and require the signature of the party or parties thereto in terms of South African law. The list does not amount to a *numerus clausus*, as there may well be other documents that the writer has overlooked.

5.2.1 A Lease together with an option to renew which exceeds 10 years -	s1 of The Formalities in respect of Leases of Land Act 18 of 1969
5.2.2 A deed of sale -	s 2(1) Alienation of Land Act 68 of 1981
5.2.3 A deed of suretyship -	s 6 of the General Law Amendment Act 50 of 1956
5.2.4 A deed of executory donation -	s 6 of General Law Amendment Act 50 of 1956.
5.2.5 A Trust deed -	s 1 of the Trust Property Control Act 57 of 1988
5.2.6 A Will or codicil -	s 52 of the Wills Act 7 of 1953
5.2.7 A Credit Agreement-	s 5(1) & (2);The Credit Agreements Act 75 of 1980
5.2.8 A Mortgage Bond -	s 50(1) of the Deeds Registries Act 47 of 1937
5.2.9 An Antenuptial contract -	s 87 of the Deeds Registries Act 47 of 1937
5.2.10 A Notarial Bond -	s 61 of Deeds Registries Act 47 of 1937.
5.2.11 A Negotiable Instrument -	ss 52, 87 & 95 of The Bills of Exchange Act 34 of 1964

In addition to the above documents, the provisions of section 12 of the Stamp Duties Act 77 of 1968 must be complied with in order to tender certain types of document as evidence for the purposes of enforceability. Revenue stamps can only be affixed to a paper document

that may contain the terms and conditions of a contract, not a stored electronic file. The section stipulates that

> " No instrument which is required to be stamped under this Act shall be made available for any purpose whatever unless it is duly stamped, and in particular shall not be produced or given in evidence or be made available in any court of law."

Examples of an "instrument" as defined by the Act would include a power of attorney or a written agreement of lease as well as documents prescribed to be in writing by other Acts mentioned above, such as a credit agreement or an antenuptual contract. Any contract requiring stamp duty would have to be in written form and contained in a document onto which revenue stamps in the requisite sum are affixed. An instrument that is not properly stamped simply cannot be tendered in evidence.

Certain of the documents mentioned above are unilateral acts and would not require consensus *ad idem* between two or more parties. They are thus irrelevant to this discussion. However any Internet contract which purported to amount to any of the abovementioned documents would be subject to the formalities imposed by legislation and would, it is submitted, by reason of the failure to comply with the requisite formalities, be held invalid. In Johnson v Leal 1980 (3) S.A.97 (A) the Appellate Division held that the failure for non-compliance with the then Act 71 of 1969, which prescribed that a deed of sale of immovable property must be in writing, was that the contract was null and void.

However, the enquiry would not end at that point. The court may well be called upon to consider the validity of a contract entered into via the Internet, in a hypothetical example, where the purported contract does not fall into the abovementioned non-exhaustive list. The court may well be called upon to decide whether the purported contract was verbal or written.

5.3 What is a written contract?

In terms of Sec. 2. (1) of the Alienation of Lands Act, a contract for the sale of land can be entered into by "the agents acting on written authority". Kerr contends that the form of authority involves two aspects:

5.3.1 The grounds of authority must be in writing

5.3.2 The writing must be authenticated as that of the principal.

Kerr contends that whilst the signature is needed on the contract itself, nothing is said in the Act about a signature being necessary for the authentication of the agent's written authority.[19] All kinds of cases have developed to support his contention that a signature is not required to authenticate the grounds of authority. It is submitted that notwithstanding the restriction of the decided cases to an interpretation of the Alienation of Lands Act, they contain reasoning which would be critical to the validity and enforceability of an Internet contract since it too has no signature appended thereto. As such, the decided cases are highly persuasive as to the analogous position of a data transmission for the grounds set out below.

5.3.3 In Balzan v O'Hara and Others, 1964 (3) S.A. (T), Coleman J. held that a telegram could constitute written authority within the meaning of the then applicable Section 11 of Act 68 of 1957, the wording of which is identical to the current act. Although in that case the original telegram form which the Seller signed was not placed before the Court, Coleman J inferred that the Seller himself had signed it himself, having taken judicial notice of the form in use for completion by the sender of a telegram, thereby inferring that the Seller had appended his signature on that form against the words "signature of sender". Coleman J however drew distinction between a telegram that is written and signed by a sender and a phonogram that is not and considered that the latter did not amount to written authority.

5.3.4 In Hugo v Gross 1981 (1) S.A. 154 (C) Freeman, J, as he then was, had to deal with the validity of the contract in terms of the Alienation of Land Act 68 of 1981, in particular Section 2 of the Act which dealt with the Agent acting on written authority. At page 160 the learned Judge found authorities suggesting that telegram emanating from a phonogram as opposed to a telegram does not constitute written authority for the Act, referring to the cases of Balzan v O'Hara and Others, 1964 (3) S.A. (T) and Meyer v Kerner 1974 S.A. 90 (N).

At 161 H to 162 G the learned Judge commented that the phonogram in the case consisted of the principal phoning a message to the post office and it had ultimately being delivered to the agent in a written form. He cited with approval the reference by Kerr to the effect that an agent would have sufficient authority if the principal were to write out authority and to hand the document to the agent with the words "there is your authority. Please offer the property to x today."

---

[19] A J Kerr the Law of Agency 3rd Edition, Butterworths 1991 at page 63

This would be an example of a written authority which is authenticated but which is not signed by the principal. At 163 A, the learned Judge held that the agent was in possession of a written authority that emanated from his principal

The learned Judge placed reliance on the uncontested evidence of the agent to the effect that she had dictated the wording necessary for the phonogram to the principal who was in Canada. The principal then in turn telephoned through the contents of the phonogram to the post office authorities in Canada, containing that exact wording. The learned Judge placed reliance on the phonogram emanating from Calgary, Canada, where the principal was at the time.

5.3.5 In Craib v Crisp 1984(3) SA 594 (T) Preiss J, had to decide on the following facts. The owner of two erven mandated an estate agent to find a Purchaser for the said erven. The estate agent introduced the Applicant to the erven whereupon a written offer to purchase was signed by her. While the offer made provision for the Seller's signature as acceptor, the Seller signified her acceptance by telegram to her mandated estate agent. At 298 C the Court held that an offer contained in one document signed by the Purchaser could validly be accepted by means of words to that effect contained in another document. At 299 A Preiss J. dealt with criticisms in respect of the authorities to the effect that the sending of a telegram would constitute a valid acceptance.

He commented on De Wet and Yates assertion in Die Suid Afrikaanse Kontrakte en Handelsreg 4th Edition at 283 to the following effect:

> "Nog minder kan did aanvaar word dat 'n telegram 'n skriftelike stuk is soos deur die voorskrif vereis. Dit bly 'n boodskap waardeer tussen persoon oorgedra moet word. "

Preiss, J. differed with the learned authors and referred to the decision in Hirsch v Nel The learned Judge analysed the telegram which was sent and noted from the body of the telegram that it emanated from Crisp. He commented at 600 G that it would be legitimate to look at the signature and particulars of the sender on the telegram at the foot of the form in order to have clarity as to the identity of Crisp. However he stated clearly that one should regard the writing at the foot of the form as being not nearly indicative of a request rather an instruction. The learned Judge contended that:

"The wording of the telegram when viewed as a whole is indicative of no less than an act on the part of the Seller to accept the written offer of which she had become aware and to ensure that acceptance be communicated to the Purchaser in order that a binding Deed of Sale should come about." at 600 H

5.3.6 In Van der Merwe v DSSM Boedery B.K. 1991 (2) S.A. 320 (T), an offer to purchase property was signed by the Purchaser and by the husband of the Seller in the Seller's presence and on the Seller's behalf. The estate agent completing the printed Offer to Purchase filled in under the heading "Seller" the name of the Seller's husband and the words "acting on behalf of in the sale of the undermentioned property." It was held that this was an unconventional, however valid method of establishing the agent's authority in writing and it satisfied the requirements of written authorisation prescribed by Section 2 of the Act. Evidence showed that the words were intended to be the Seller's authorisation of her husband to act on her behalf. The estate agent had filled in the Applicant's name followed by the words "acting on behalf of" (Appellant's wife in the sale of the abovementioned property). The Court found that the Applicant had not qualified his signature to indicate his representative capacity therein but that the words "acting on behalf of" was legally sufficient representation of his authority.

5.4 Was the document signed or not?

In Putter v The Provincial Insurance Co. Ltd and another 1963 3 SA 145 (W) Coleman A.J, as he then was, considered the validity of a thumb print made as a mark to identify a statement. The issue before the court was whether or not the thumb print constituted a signature within the meaning of Sec. 2(4) of the Evidence Act 14 of 1962 making it admissible. At 148 A the learned Judge held that a signature ordinarily takes the form of a person's name written by him on the document, but this is not the acceptable form of a signature. The learned Judge indicated that the verb "to sign" derives from the Latin word "signum", which he considered to relate more to a "mark" than the conventional written understanding of the word.

He then referred to the Webster's dictionary definition and other decided cases which in his learned opinion provided for the extension of the conventional criteria of the meaning of sign to include to mark or seal, to represent or indicate by a sign or ratify or a test by hand or seal. The learned Judge held that the thumbprints made by Mrs Makenna identified the documents as hers and therefore held that the document was signed by her within the meaning of Sec. 2(4) of the Evidence Act.

5.5 How does this apply to an Internet contract?

An Internet contract would not be signed in the conventional sense of the meaning of "signature" and the party relying on a data transmission would bear the onus of establishing the admissibility of the data message. This could only be established by relying on the Computer Evidence Act 57 of 1983 as amended by The Amendment Act 5 of 1992

Chris Reid[20] identifies the two potential areas of dispute

5.5.1. Where the sender denies that the message stored on the recipient's computer is actually sent by him,

5.5.2 Where he admits that he sent a message, but denies that the contents of the message stored on the recipient's computer correspond with the message sent.

The author highlights the problem with e-mail and by implication any communication sent via the Internet.

> "Where signed physical documents exist they can be produced to prove the fact of sending and the contents of the message. The sender's physical signature will prove that he sent it and in any alteration to its content should be apparent on its face. The problem with electronically stored messages is that alteration is simple and leaves no traces. Unless these messages can be well authenticated as physically signed documents the use for contract formation or other transactions will remain at best highly problematical."

He noted however, referring to South African legislation that

> "The Computer Evidence Act of 1983 allows the admission of computer records as evidence without imposing any special technical conditions, the Court deciding what weight is to be appropriate to be given to the evidence."

5.6 Computer Evidence Act 57 of 1983

In terms of section (7) (3) of the Act an "authenticated computer print-out

> "(1) In any civil proceedings... shall be admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible.
> (2) ...If an affidavit which accompanies the computer print-out in question as contemplated in the definition of 'authenticated computer print-out' in section 1 (1), on the face of it complies with the provisions of section 2 which apply to an affidavit of the nature in question".

The deponent to such an affidavit would be required to state that "to the best of the deponent's knowledge and belief "

---

[20] Chris Reid "Authenticating electronic mail messages, some evidential problems" Modern Law Review Vol. 52 Sept. 1989, 649

"[he] is qualified to give the testimony it contains by reason of-

(a) his knowledge and experience of computers and of the particular system by which the computer in question was operated at all relevant times; and

(b) his examination of all relevant records and facts which are to be had concerning the operation of the computer and the data and instructions supplied to it."

The deponent would be required to state under oath that the printout

> "... comprise [s] all the relevant records and facts which are to be had concerning the operation of the computer in question and the data and instructions supplied to it".

Clearly, the Act provides for the admissibility of written testimony of a system administrator or information systems supervisor in an organisation since such a person's knowledge and experience would be difficult to refute. However the Act makes no mention of private individuals who merely understand how to use a personal computer. The Act is silent on the degree of knowledge and experience a deponent must have for the affidavit to be admissible.

5.7 Can A Private Individual Depose To An Affidavit?

It is therefore submitted that the Act does not preclude a non-professional computer user provided that he is sufficiently technologically literate to understand the mechanics of the operating system of the computer, as well as the application by which an Internet contract is originally prepared as well as the application by which the Internet contract is transmitted, if the two are separate applications.

However, no rule can be identified since the casuistic approach in South African law permits a judicial officer to exercise his discretion in the circumstances of each matter which appears before the court. Consequently the admissibility of affidavit evidence would depend largely on background provided in the affidavit itself and the annexures thereto, which may or may not include, inter alia:

5.7.1 The deponent's familiarity with the operating system;

5.7.2 The deponent's familiarity with the application;

5.7.3 The deponent's experience of information technology;

5.7.4 The technical specifications of the computer or server on which the Internet contract was generated;

5.7.5 Technical information on the period of time which the operating system and applications had been installed on the computer or server;

5.7.6 Logs or transmission records of messages transmitted by the computer;

5.7.7 Logs or transmission records of messages received by the computer.

Where the deponent's "expertise" is established, the printout which is relied upon should be significantly similar if not identical to contents of the data message as it appeared on the computer monitor at the time that the data message was received or transmitted. For example, it is submitted that accepting an offer, together with a printout of a confirmatory delivery notification would, *prima facie*, be admissible to prove the fact of receipt of acceptance.

5.8 Printouts of E-mail Messages

The New Zealand Law Commission Working Group remarked that

> "Many communications software packages allow the sender of a message to check whether a message has been received or read. Although the legal effect of such features is as yet untested, they may at least provide evidence that the offeree has had access to a message."[21]

As a general rule, it is further submitted that there would be no basis to deny the admissibility of such a form of acceptance, irrespective of whether or not the offer purporting to be accepted was made in person, by post, telephone, telegram. telefax or initiated by e-mail provided that no mode of acceptance is prescribed in the offer and subject to all general principles of contract.

5.9 Testimony from A Third Party

Where an intermediary such as an ISP or a WAN node is involved, the deponent cannot testify as to the information system of that intermediary since that falls outside of the scope of the deponent's knowledge. Nevertheless, he or she could depose to the history, nature and scope of the relationship with the intermediary and to the reliability of receipt and transmissions of e-mail. Where further evidence that can only be provided by an intermediary is required, the Act allows that

> "S (7) An authenticating affidavit [which] shall be supplemented by-
> (a) such further affidavits as are necessary for substantial compliance with subsections (1) to (6) when that is not achieved without them;

---

[21] The New Zealand Law Commission report on Electronic Commerce at pg.84 <http://www.lawcom.govt.nz/pub_index.html >

(b) any additional affidavits the circumstances may require."

It is therefore submitted that the Act would allow the affidavit of an intermediary to prove the fact of transmission provided that the system integrity of intermediary was sufficient to confirm with the requirements relating to the production of a printout to certify that the intermediary's mail server was-

> "s 2 (1) (d) (i) correctly and completely supplied with data and instructions appropriate to and sufficient for the purpose for which the information recorded in the computer print-out was produced;[and]
> (ii) unaffected in its operation by any malfunction, interference, disturbance or interruption which might have had a bearing on such information or its reliability;"

As a matter of commercial practice, any professional intermediaries who fell short of this standard would not be able to provide its service to its clients. Therefore, the standard set by the Act accords with reality. Where an intermediary for some reason is not able to provide a supplementary affidavit, ie where it is no longer in operation, the court can exercise its discretion to admit the evidence contained in the main affidavit and decide at a later stage what weight should be placed on the evidence.

5.10 The Court's Discretion To Admit Hearsay Evidence

The court can be invited to exercise its discretion in terms of section 3 of the Law of Evidence Amendment Act 1998 to allow what would be considered, provided that the "person on whose credibility the probative value depends...testifies at such proceedings." The court may provisionally decide to accept documentary evidence to show that a data message was sent or received provisionally, even without a verifying affidavit, provided that the network administrator of the intermediary testifies in the same proceedings to establish the veracity and authenticity of the particular data message in question.

Whether or not the network administrator or technical manager of the ISP concerned will be able to establish the underlying foundation of the data message depends entirely on the extent to which adequate records and logs which would form the basis of an audit trail have been kept. Clearly, this will be a question of fact that may vary as between intermediaries as no regulations or legislation prescribes the manner and form of records or logs that must be maintained.

Where the admissibility of the affidavit is established, the court is further authorised to exercise its discretion as to the weight that it shall, in the applicable circumstances, apply to the affidavit, where such an affidavit is tendered in evidence.

> "4 Evidential weight of authenticated computer print-outs
> (1) An authenticated computer printout shall have the evidential weight which the court in all the circumstances of the case attaches to it.
>
> (2) In order to assess the evidential weight of an authenticated computer printout, the court may-
>
> (a) take account of anything contained in the authenticating affidavit or a supplementary affidavit;
>
> (b) on the application of any party to the proceedings require the deponent to the authenticating affidavit or a supplementary affidavit or any other person to testify orally on any topic relevant to such question, whether or not any such affidavit covered it."

5.11 Reliance on an Internet Contract.

Where a party tenders evidence which conflicts with statutory provisions, it will not be admitted. Yet there is no decided case or statute, that, in itself, precludes an Internet contract on the mere grounds of it being concluded via the Internet

The party relying on an Internet contract must adduce evidence to establish the validity and enforceability of an Internet contract. Therefore, such parties should set their evidence within the four corners of the relevant Acts, in order for the grounds on which they are relying even to be considered by the court.

Part Two

Chapter Six - Application of Decided Cases to Internet Contracts

6.1 What Category of Communication does E-mail Fall Into?

6.1.1 Are the Principles Applicable to Telefax or Telephone Communication Relevant?

Paula Bagraim contends that an e-mail communication differs from a fax or telephone communication in two ways.[22] There is no direct line of communication between sender and receiver; rather e-mail is broken into packets, each with an address for the recipient. She maintains, correctly, that e-mail can be misaddressed, delayed and not collected for some time after delivery. On a dedicated circuit ie a telephone call, it is possible to verify immediately that the intended recipient has heard the acceptance. With e-mail, this is more difficult. For this reason, the author contends that it is difficult to verify that the offeror has received an unequivocal acceptance.

6.1.2 Analogy to Electronic Data Interchange (EDI) Communications: Invoking the Expedition Theory where no instantaneous link exists

Chris Reid contends that where acceptance is made by some instantaneous means, such as face to face communication or telephone, it must actually reach the offereror.[23] The author contends that the rule applicable to telex communications, ie. that contracts made by telex are made where the telex is received is applicable to EDI where there is a direct link between the parties. This may be applicable to an Internet contract where one or more parties has permanent connectivity via a dedicated diginet link.

He contends further that the position may be different if the network across which the message is transmitted stores the acceptance message for an appreciable period before it is delivered to the offeror. He posits further whether the postal rules may apply to such an EDI message of acceptance and mentions two justifications for invoking the postal rule in such circumstances.

He cites the obiter dictum of Lord Brandon of Oakbrooke in the Brinkibon case at page 48

> "[T]hat reasons of commercial of expediency apply to cases where there is bound to be a substantial interval between the time when acceptance is sent and the time when it is received. In such cases the exception to the general rule is more convenient and makes on the whole for greater fairness than the general rule itself would do."

---

[22] "Contracting in Cyberspace" Juta's Business Law 1998 Vol. 6 part 2. pg. 54

[23] Computer Law 3rd edition Blackstone Press 1990 pg.304

The author contends that the second justification for the postal rule being applicable to EDII acceptances is that the offeror has impliedly agreed that the accepting party may entrust the transmission of acceptance to an independent third party, analogous to the postal authorities. He contends that application of this doctrine would suggest that acceptance takes place when the message is received by the system provider's computer.

He suggests that the clearest analogy to using a store-and-forward EDI system (which operates on a similar mechanism to e-mail) is with acceptance by telegram. Since it is necessary for the message actually to be communicated to the telecommunication service, normally by telephone, thus once received by the service, acceptance is complete.

The author contends that if the postal rule applies, the time of acceptance is the time the EDI message was received and the place of acceptance will therefore be at the node of the network which received the message. While in most cases this is likely to be in the same jurisdiction as the acceptor, there may be circumstances when the network node receiving the acceptance is not in the same jurisdiction as the originating offer made via EDI.

6.2 Is an Internet contract formed instantaneously?

The New Zealand Law Commission Working Group cautions against classifying acceptance of an offer using electronic communications as one that falls within the general ambit of an instantaneous communication at all. It proposes that, in cases involving a facsimile transmission, it is likely that the court will hold that there has been an instantaneous communication to the machine of the offeror in the same way that a telex communication was viewed as an instantaneous communication in both Entores and Brinkibon. [24]

If this "instantaneous communication" reasoning is extended to communication made by e-mail, the fact of whether or not the transmission was instantaneous or delayed may well conflict with such reasoning.

6.3 Direct or Indirect Link

The Commission contends that it would depend on whether the e-mail user had direct and immediate access to the person to whom the e-mail is sent or whether the e-mail was sent

[24] idem supra n 21 at pg.48

through the electronic equivalent of the postal service, an internet service provider (ISP), which collected the mail. [25]

> "Users in the former category have a mode of communication which is close to instantaneous while those using an ISP may only communicate as quickly as their telephone access, service provider and personal inclination dictate."

As the Commission noted, the complexity increases when the issue of the offeror's right to revoke the contract by notice to the offeree is raised, where such notice is given electronically. The offeree may choose to accept and bind the offeror to the terms of the offer at any time until the revocation is effective, regardless of whether the offeror still wishes to enter into the contract. They posit

> "Is the offer revoked when a message arrives at the offeree's ISP; or when the offeree collects his or her mail from the ISP; or when the offeree actually reads the notice? "

The Commission listed the following three factual issues, are all outside the control of the offeror which clearly complicate the legal position.

6.3.1 Whether the offeree has direct or indirect access to the message (ie, whether e-mail or other communication is delivered directly to the offeree or whether the offeree must take steps to collect messages, such as dialing his or her ISP);

6.3.2 Whether the offeree is experiencing problems in receiving incoming messages (for reasons outside the control of the offeree, such as a power failure); and

6.3.3 The existence of a time difference between offeror and offeree.

The same uncertainties relate to the right an offeror to withdraw an offer at any time before the acceptance is communicated. [26] The uncertainty caused by the relevant technology may cause a dispute when a delay subsequently enables the offeror to either revoke the offer, or argue that it has lapsed.

If it is assumed that the expedition theory may not be appropriate, or that it does not apply, it would be possible for an offeree to e-mail his or her acceptance, then decide to withdraw acceptance in a separate e-mail sent later, and for the offeror to receive both these messages at the same time. If the expedition theory applied when acceptance is sent electronically, acceptance cannot be revoked.

---

[25] at pg. 49
[26] at pg.54 idem supra n 21

6.4 Legislation to clarify the common law position

To avoid uncertainty and in the absence of a decided case, deeming provisions could be only be invoked by legislation to hold a message to have been received either at the time it was sent, or at the time it would ordinarily be received but for circumstances outside the control of the parties.

In considering what legislation may be most suitable it may be logical to consider what existing instruments are relevant to contracting in general.

6.5 International Instruments

6.5.1 The Vienna Sales Convention

Article 24 provides:

> "For the purposes of this Part of the Convention, an offer, declaration of acceptance or any other indication of intention "reaches" the addressee when it is made orally to him or delivered by any other means to him personally, to his place of business or mailing address or, if he does not have a place of business or mailing address, to his habitual residence."

In terms of a wide meaning of "mailbox", an offer made by e-mail would reach the offeree at the time it entered his or her mailbox, at the network node. There is no requirement under the Vienna Sales Convention that the intended recipient be subjectively aware of the existence of a message.

This approach is consistent with the approach taken in article 15 of The Model Law on Electronic Commerce (hereinafter referred to as "the Model Law")[27], as are the approaches adopted by the Legislatures of the United States and Singapore. Although the Australian approach differs slightly, depending on whether the recipient has designated an information system for receipt, the provisions of all three countries are similar.

6.6 Domestic Legislation

6.6.1 Australian Law

The 1998 report of the Australian Electronic Commerce Expert Group, recommended the enactment of rules on the timing of messages to avoid confusion, and that receipt should occur when the recipient is able to retrieve the message in a form which his system is

---

[27] <http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm>

capable of processing, unless he designates an information system for receipt. [28] The message would be received at the time when it comes to the attention of the addressee, in terms of a recommended fallback position. Where an information system is designated by the recipient , receipt occurs when the electronic communication enters that information system, after dispatch of the electronic communication by the sender. This recommendation forms part of the current Bill. [29]

6.6.2 United States Federal Law

Article 2B section 2-213(b) of the Uniform Commercial Code provides that electronic messages are effective on receipt, regardless of whether any individual is aware of receipt.[30]

"Receipt" is defined in the article 2B, section 2-102

> "when it enters an information processing system in a form capable of being processed by a system of that type and the recipient uses or has designated that system for the purpose of receiving records or information.

6.6.3 Singapore Law

The Electronic Transactions Act 1998 defines receipt as follows:[31]

"15. Time and place of despatch and receipt

(1) Unless otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters an information system outside the control of the originator or the person who sent the electronic record on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs
at the time when the electronic record enters the designated information system; or

i. if the electronic record is sent to an information system of the addressee that is not the designated information system, at the time when the electronic record is retrieved by the addressee;"

Since the Model Law appears to be the basis of deeming provisions which have been invoked by legislation, it merits more detailed analysis.

---

[28] Electronic Commerce: Building the Legal Framework, (para 4.5.8–90) <http://www.law.gov.au/aghome/advisory/eceg/single.htm>

[29] Electronic Transactions Bill 1999 < http://law.gov.au/ecommerce/DraftBill/DraftBill.pdf> see below Chapter Eight, pg. 49

[30] Article 2B section2-213(b) of the Uniform Commercial Code <http://www.law.upenn.edu/library/ulc/ucc2/2b398.pdf> see below Chapter Twelve, pg. 57

[31] <http://www.cca.gov.sg/regulations/framecontent.html> see below Chapter Nine, pg. 51

Part Three

Chapter Seven The Uncitral Model Law on Electronic Commerce

7.1 The Uncitral Model Law on Electronic Commerce

The Model La is divided into two parts: the first deals with electronic commerce generally while the second deals with electronic commerce in specific areas (carriage of goods and transport documentation) as well as a Guide to Enactment: (hereinafter referred to as "the Guide") This dissertation only deals with the first part concerning electronic commerce and the Guide.

The Model Law is intended to be a "general tool for executive branches of Governments and legislators modernising their legislation to, inter alia:

> ".., offer national legislators a set of internationally acceptable rules..;"
>
> "...create a more secure legal environment for electronic commerce...,"
>
> "...be of use to individual users of electronic commerce in the drafting of some of the contractual solutions that might be needed to overcome the legal obstacles to the increased use of electronic commerce"
>
> "...permit States to adapt their domestic legislation to developments in communications technology applicable to trade law without necessitating the wholesale removal of the paper based requirements themselves or disturbing the legal concepts and approaches underlying those requirements, [accepting]...that the electronic fulfillment of writing require[s] amendments [and] might, in some cases, necessitate the development of new rules."

The Model Law was prepared due to one of the many distinctions between EDI messages and paper based documents, namely, that the " latter were readable by the human eye, while the former were not so readable unless reduced to paper or displayed on a screen."

7.2 Functional Equivalence and Technology Neutrality

The Uncitral Model Law relies upon functional equivalence (also know as media neutrality) and technology neutrality.[32]

The term functional equivalence means that transactions conducted using paper documents and transactions conducted using electronic communications should be treated equally by the law and not given an advantage or disadvantage against each other. Technology neutrality means that the law should not discriminate between different forms of technology - for example, by specifying technical requirements for the use of electronic communications

that are based upon an understanding of the operation of a particular form of electronic communication technology. [33]

Objective 17 elaborates on the basis for this approach.

> "A data message, in and of itself, cannot be regarded as an equivalent of a paper document in that it is of a different nature and does not necessarily perform all conceivable functions of a paper document."

To implement the "functional-equivalent" approach, the working groups had to consider

> "the various layers of existing requirements in a paper-based environment:, ...[and] the existing hierarchy of form requirements, which provides distinct levels of reliability, traceability and inalterability with respect to paper-based documents."

7.3 Scope of Applicability of the Model Law

Objective 7 defines the scope of applicability of the Model Law to govern

> " communication by means of EDI defined narrowly as the computer-to-computer transmission of data in a standardised format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission of free-formatted text by electronic means, for example through the INTERNET. It was also noted that, in certain circumstances, the notion of "electronic commerce" might cover the use of techniques such as telex and telecopy"

This extension was considered necessary to cater for

> "situations where digitalized information initially dispatched in the form of a standardised EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of a telecopy of a computer print-out. A data message may be initiated as an oral communication and end up in the form of a telecopy, or it may start as a telecopy and end up as an EDI message."[34]

7.4 Current Status of Adoption of the Model Law

Legislation based on the Uncitral Model Law on Electronic Commerce has been adopted in the Republic of Korea, Singapore and, within the United States of America, Illinois as at 23 March 1999.[35]

---

[32] <http://www.lawcom.govt.nz/pub_index.html> at pg. 28
[33] set out in Objective 6 of the Guide
[34] Objective 7 and 8 of the Model Law
[35] United Nations Office of Legal Affairs servicing the United Nations Commission on International Trade Law (UNCITRAL) STATUS OF CONVENTIONS AND MODEL LAWS
<http://www.un.or.at/uncitral/english/status/status.pdf>

In January 1999 the Australian Attorney-General's Department submitted its draft Electronic Transactions Bill of 1999 to Parliament. It is based on the Model Law to a large extent with the exception of certain articles discussed in more detail below.[36].

In the United States, Article 2B of the Uniform Commercial Code dealing generally with sale has been amended on repeated occasions to allow for the application of traditional concepts to electronic contracting. The latest amendment dated March 1998 sets out guidelines for electronic contracting.[37]

The Model Law was influenced by United States legal developments in its inception, early stages, and final articulation. In turn, the Model Law itself has had significant influence on revision efforts within the United States, even before its finalisation in 1996. [38] The reason for what has been referred to as "symbiosis" may lie in the historic relationship between Uncitral and the Drafting Committee on the Uniform Electronic Transactions Act (UETA). A strong working relationship had been established prior to and during the drafting and ratification of the Vienna Convention in 1980. The Vienna Convention is considered to be the functional equivalent of Article 2 of the Uniform Commercial Code and the provisions of the two are similar.

The Model Law, which was influenced by United States developments has adopted in other non-uniform electronic commerce legislation proposed in the states of Illinois and Massachusetts; in their promulgation of electronic signature or digital signature legislation This is discussed in more detail below in Chapter Twelve.

To date South Africa has not enacted any similar legislation or White paper to Parliament but South Africa was represented in observer status at the recent session of the Working Group on Electronic Commerce. In addition the session was attended by observers from the following States: Angola, Belarus, Belgium, Bolivia, Canada, Croatia, Cuba, the Czech Republic, Georgia, Guatemala, Indonesia, Ireland, Kuwait, Lebanon, Morocco, the

---

[36] <http://law.gov.au/ecommerce/expaper.pdf>
[37] <http://www.law.upenn.edu/library/ulc/ucc2/2b398.pdf>
[38] Amelia H. Boss Tulane Law Review June, 1998 72 Tul. L. Rev. 1931 "Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform" The page number of this reference cannot be provided as the article was downloaded from <http://www.web.lexis-nexis.com/universe/form/academic/univ_lawrev.html>, and no page numbers were provided in the text

Netherlands, New Zealand, Poland, Portugal, the Republic of Korea, Saudi Arabia, Slovakia, Sweden, Switzerland, Turkey, and Uruguay.[39]

7.5 The Provisions of the Model Law

Part One of the Model Law, "Electronic commerce in general" consists of three chapters and fifteen articles.

Chapter I. General provisions

7.5.1 Article 1. Sphere of Application

This article affords States the alternative of applying the Model Law to "any kind of information in the form of a data message used in the context of commercial activities" or to limit the applicability of the Law to a data message relating only to "international commerce."

7.5.2 Article 2. Definitions

The Model Law clarifies the position of potential contacting parties by setting out definitions which in themselves ascribe no contractual status to parties but which rather focuses on the nature of the interaction between them.

> "a) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; ...
>
> (c) "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;
>
> (d) "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message; "

The Model Law does not refer to offeror or offeree but rather of an originator and addressee. The "addressee" under the Model Law is the person with whom the originator intends to communicate by transmitting the data message, as opposed to any person who might receive, forward or copy the data message in the course of transmission. The "originator" is the person who generated the data message even if that message was

---

[39] Report Of The Working Group On Electronic Commerce On The Work Of Its Thirty-Fourth Session (Vienna, 8-19 February 1999) <http://www.un.or.at/uncitral/english/sessions/unc/unc-32/acn9-457.htm>

transmitted by another person. The definition of "addressee" contrasts with the definition of "originator", which is not focused on intent.

> "(e) "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message; '

The purpose of identifying a third party would be to cater for additional value-added services which may be performed by network operators and other intermediaries, such as formatting, translating, recording, authenticating, certifying and preserving data messages and providing security services for electronic transactions. The Model Law, which is focused on the relationships between originators and addressees, does not, in general, deal with the rights and obligations of intermediaries.

7.5.3 Article 3. Interpretation

The Model Law is intended to be enacted as part of domestic legislation and therefore domestic in character, yet the Guide stresses that it should be interpreted with reference to its international origin in order to ensure uniformity in the interpretation of the Model Law in various countries.

The guide to the Model Law proposes the following non-exhaustive list in consideration thereof:

> "(1) to facilitate electronic commerce among and within nations;
> (2) to validate transactions entered into by means of new information technologies;
> (3) to promote and encourage the implementation of new information technologies;
> (4) to promote the uniformity of law; and
> (5) to support commercial practice"

7.5.4 Article 4. Variation by agreement

The provisions contained in chapter II of part one are regarded as mandatory as they amount to what was considered as the "minimum acceptable requirement'. The Model Law aims to support the principle of party autonomy by allowing the provisions of chapter III of part one to be varied either by bilateral or multilateral agreements between the parties, or by system rules agreed to by the parties. The Model Law provides that these articles may only be modified by agreement to the extent that that would be permitted by national law.

The reason for the distinction is founded on a concern that

> "an unqualified statement regarding the freedom of parties to derogate from the Model Law might thus be misinterpreted as allowing parties, through a derogation to the Model Law, to derogate from mandatory rules adopted for reasons of public policy., unless expressly stated otherwise." [40]

The text expressly limits party autonomy to rights and obligations arising as between parties so as not to suggest any implication as to the rights and obligations of third parties.

7.5.5 Chapter II. Application of legal requirements to data messages

7.5.5.1 Article 5. Legal recognition of data messages

By stating that "information shall not be denied legal effectiveness, validity or enforceability solely on the grounds that it is in the form of a data message", article 5 states that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability.[41]

7.5.5.2 Article 5 bis. Incorporation by reference

In June 1998, the above article was adopted by the Commission at its thirty-first session and extended recognition to information not contained but merely referred in the data message purporting to give rise to legal effect.

The reason for this extension is to avoid

> "...an obligation to overload,... data messages with quantities of free text when [practitioners] can take advantage of extrinsic sources of information, such as databases, code lists or glossaries, by making use of abbreviations, codes and other references to such information."

Incorporation by reference into other data messages was seen as essential to the use of public key certificates, since certificates are "brief records with rigidly prescribed contents that are finite in size". The certificate authority which issues the certificate, however, is likely to require the inclusion of relevant contractual terms limiting its liability which cannot occur without external terms being incorporated by reference.[42]

---

[40] the Guide clause 45
[41] the Guide clause 46

7.5.6 Article 6. Writing

The Model Law defines a basic standard to be met by a data message in order to be considered as meeting a requirement (which may result from statute, regulation or judge-made law) that information be retained or presented "in writing".

7.5.7 Article 7. Signature

Paragraph (1)(a) establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of a data message and confirms that the originator approved the content of that data message.

Paragraph (1)(b) establishes a flexible approach to the level of security to be achieved by the method of identification used under paragraph (1)(a). The method used under paragraph (1)(a) should be as reliable as is appropriate for the purpose for which the data message is generated or communicated, in the light of all the circumstances, including any agreement between the originator and the addressee of the data message.

Rather than attempt to set out a comprehensive code encompassing all aspects of electronic signature infrastructure, use and technology, article 7 states that an electronic signature may be as legally effective as a manual signature, but does not define an electronic signature.[43] The Model Law is silent on the form an electronic signature may take. It does not necessarily require the implementation of an infrastructure for issuing signatures. It is more concerned with the issue of whether a particular electronic signature met a legal requirement of signed writing.

7.5.8 Article 8. Original

Article 8 states the minimum acceptable form requirement to be met by a data message for it to be regarded as the functional equivalent of an original, ie where

> " (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
>
> (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented. "

---

[42] the Guide clauses 46-2 and 46-3

[43] the Guide clauses 56 and 57

The Guide contends that " If "original" were defined as a medium on which information was fixed for the first time, it would be impossible to speak of "original" data messages, since the addressee of a data message would always receive a copy thereof."[44]

Article 8 contains robust criteria for determining data integrity

> " [3] (a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and
>
> [3] (b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

7.5.9 Article 9. Admissibility and evidential weight of data messages

Article 9 seeks to establish both the admissibility of data messages as evidence in legal proceedings and their evidential value. With respect to admissibility, paragraph (1) establishes that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form.

Paragraph (2) provides useful guidance as to how the evidential value of data messages should be assessed (ie, depending on whether they were generated, stored or communicated in a reliable manner).

7.5.10 Article 10. Retention of data messages

> "(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:
>
> (a) the information contained therein is accessible so as to be usable for subsequent reference; and
>
> (b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
>
> (c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received. "

---

[44] clause 62

All three conditions must be met. Subparagraph (c), imposes a standard for the retention of the transmittal information associated with the data message, arguably higher than as to the storage of paper-based communications.

Chapter III. Communication of data messages

7.5.11 Article 11. Formation and validity of contracts

This article states that an offer and the acceptance of an offer may be expressed by means of data messages.

7.5.12 Article 12. Recognition by parties of data messages

This article relates to communication not intended to bring a contract into existence by stating that "a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message".

7.5.13 Article 13. Attribution of data messages

Article 13(2) provides that a data message is attributable to a party if it was sent by an authorized agent of the party, or by an information system programmed by, or on behalf of, that party to operate automatically These provisions are intended to resolve issues arising from the need to attribute an electronic message to a party for evidential purposes, and to protect those who act in reliance upon such messages.

7.5.14 Article 14. Acknowledgement of receipt

This article sets out rules that apply "where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged."

7.5.15 Article 15. Time and place of dispatch and receipt of data messages

This article provides rules for timing and the place of dispatch and receipt of electronic messages: This provision eliminates the confusion caused by the possible application of the postal acceptance rule by deeming messages to be received when they enter the addressee's designated information system.

There is no allocation of risk for messages which are illegible; nor is there any provision for situations where the addressee is for any reason unable to retrieve his or her mail. This is consistent with the principle of technological neutrality, as the law does not currently allocate risks for such events when communications are recorded and sent using paper.

Part Three

Chapter Eight The Australian Working Group Report

In an report to The Attorney General entitled "Building The Legal Framework", and dated 31 March 1998, The Electronic Commerce Expert Group made the following recommendations regarding implementation of domestic legislation for removing legal uncertainties, based on the Model Law.[45] It recommends recognition that information, records and signatures in an electronic form should not be denied legal effect solely on the grounds that it is in an electronic form. (Article 5 of the Model Law)

It contends that a data message should satisfy any requirements for information to be in writing and approves of the requirement in Article 6 of the Model Law for information be "accessible so as to be usable for subsequent reference" as establishing an acceptable basis upon which to develop functional equivalence.

It approves of Article 7 of the Model Law as providing an appropriate model for Australia to address the threshold issue of legal recognition of electronic signatures. However, the expert group did not make specific recommendations regarding the form of signature and expressly recommended that

> "When determining the reliability of a method of author identity and content approval, the method should be as reliable as appropriate at the time the method was used"[46]

The expert group approved of Article 8 of the Model Law and suggested provisions allowing data messages to satisfy requirements for an original, subject to requirements about the integrity of the data message.

In regard to the enforceability of electronic agreements and the admissibility and evidential weight of electronic documents or data messages, The Uniform Commonwealth and New South Wales Evidence Acts were considered sufficient to satisfy the requirements of article 9 of the Model Law, and were considered to provide an appropriate model for the other States and Territories to adopt. No further legislation in this respect was considered necessary.

Article 10 of the Model Law which prescribes a basis for the equivalence of electronic and paper based record retention requirements for storage of information as data messages:

---

[45] <http://www.law.gov.au/aghome/advisory/eceg/single.htm>
The Draft Bill based on the Recommendations is available at
<http://law.gov.au/ecommerce/DraftBill/DraftBill.pdf>

[46] Recommendation 7

accessibility; integrity; and retention of transmittal information so as to enable identification of the data message, was recommended in its entirety.

The expert group recommended provisions equivalent to the general statement of principle in article 11 of the Model Law to remove any uncertainty concerning the use and validity of data messages in contract formation.

However, the expert group were reluctant to sanction article 13 of the Model Law which allocates commercial risks between originator and addressee on the basis that such a recommendation

> " may involve incorrect guesses about efficient and fair business practices across a range of commercial contexts and may have serious unintended consequences"[47]

Article 13 was considered to move beyond the existing common law position in Australia that applies to paper-based transactions by allocating the risk of loss arising from unauthorised or altered messages to the apparent originator rather than the addressee.

The expert group approved the approach in article 15 of the Model Law, in relation to the time of dispatch of a data message and suggested that legislation deeming the time of dispatch as when the data message entering an information system outside the control of the sender. However the expert group held that the tests set out in article 15 with respect to time of receipt, have the potential to create the situation where a message may be deemed to have been received by the addressee before it was sent by the originator. And therefore recommended that all time should be referenced to Universal Time/Greenwich Mean Time.

In regard to the place of receipt they preferred

> " to rely upon the recipient's ability to retrieve the information and, as a fall back position, upon the information coming to the attention of the recipient." [48]

Therefore the expert group recommended the place of business of the parties as being the place of receipt.

The Electronic Transactions Bill 1999, presented to The House Of Representatives of the Parliament of the Commonwealth of Australia by the Australian Attorney General contains all of the above recommendations.

---

[47] Recommendation 12
[48] Recommendation 13

Part Three

Chapter Nine The Singapore Electronic Transactions Act 1998

The Electronic Transactions Act 1998 enacts the Electronic Transactions Bill of the same year. The Bill was presented to the Parliament of Singapore and contained the provisions of The Model Law, as well as detailed provisions that make provision for certification authorities and digital signatures. The President of Singapore, "on the advice and consent of the Parliament of Singapore", enacted legislation which is of broader scope and in far more detail than the Model Law although it is largely based thereon.[49]

Clause 3 explains, to some measure, the rationale for the scope of the legislation.

> " In addition to facilitating electronic commerce the legislature intends to facilitate electronic filing of documents, to minimise the incidence of fraud and to promote public confidence in the integrity, liability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures."

Clause 4 indicates that the legislation is not applicable to the creation or execution of wills, negotiable instruments, trusts, powers of attorney, contracts of sale or disposition of immovable property, or to the conveyance of immovable property or any documents of title.

Part 2 of the Act invokes word for word, clauses 5, 6,7 and 8 of the Model Law. However clause 9 of the Singapore Act sets out more detailed provision in regard to the retention of electronic records.

Part 3 of the Act provides for the liability of network service providers.

Clauses 11, 12, 13, 14 and 15 of Part 4 of the Act which deal with electronic contracts. are largely based on the Model Law.

Part 5 of the Act, dealing with secure electronic records and signatures, sets out detailed legislation, concerning the applicability and validity of electronic signatures, presumptions relating to secure electronic records and signatures.

---

[49] <http://www.cca.gov.sg/regulations/framecontent.html>

Part 6 thereof deals with the effect of digital signatures and sets out inter alia, presumptions regarding certificates, the consequences of relying on a digitally signed record.

Part 7 sets out general duties relating to general signatures and creates a criminal sanction for any person who knowingly creates, publishes, or makes available a certificate for fraudulent or unlawful use as well as a lesser fine for misrepresentation to a certification authority of identity.

Part 8 of the Act sets out the duties of certification authorities themselves and detailed procedure for the issuing of a certificate, suspension of a certificate, revocation of a certificate with or without the subscriber's consent as well as the rules relating to control of private keys.

Part 10 of the legislation provides for the appointment of a Controller of Certification Authorities for the purposes of licensing, certifying, monitoring and overseeing the Activities of certification authorities. Clause 42 thereof allows the Minister to regulate and issue licences to certification authorities.

The Controller is given broad powers, inter alia, to have access to and to inspect the operation of any computer system or associated apparatus, which he has reasonable cause to believe, has been in use with a connection with any offence under the Act.

Clause 55 authorises the Controller to require the production of records, accounts, documents and data kept by a licensing authority and to inspect, examine and to make copies of them.

Part Three

Chapter Ten[50] - The South Korean Basic Law on Electronic Commerce

The South Korean legislature has incorporated the Model Law and allow parties to electronic interchange agreements to modify articles 9 to 12 by an agreement as between them, in so doing giving effect to article 4 of the Model Law.

The legislation takes the form of a proposed Bill which contains 6 chapters and 34 articles. It contains a stipulation that the Bill becomes effective in its current form as of 1 July 1999.

The definitions clause of the South Korean legislation sets out identical definitions to those contained in the Model Law as well as provisions relating to digital signatures certification authorities.

Chapter 2 of the South Korean legislation gives effect to articles 5, 6, 9 10, 13, 14 and 15, but is silent on clauses 11 and 12 of the Model Law.

Chapter 2, Article 5 gives effect to Article 5 of the Model Law.

The South Korean Bill is silent with regard to provisions relating to article 6 of the Model Law in respect of the validity of information contained in the data message amounting to writing where required by law.

Article 6 of the South Korean Bill allows for the validity of digital signatures but prescribes that they have to be certified by the authorised certification authorities set out in article 16 of the Bill to be deemed as a valid signature or seal. Inasmuch as the Model Law refers to a method which is reliable and appropriate for linking a person to a data message, the South Korean legislation sets out mandatory requirements for such a method.

Chapter 2, article 7 of the South Korean legislation gives effect to article 9 of the Model Law by allowing the admissibility of electronic messages as evidence.

The South Korean legislation is silent with regard to article 8 of the Model Law in respect of information to be retained in an original form.

---

[50] <http://www.mbc.com/legis/south_korea.html> This section is based an English translation of South Korean legislation made available at this site

Article 8 of the South Korean legislation gives effect to article 10 of the Model Law in regard to retention and storage of documentation or records.

Article 9 sets out, verbatim, the requirements of Article 15 of the Model Law in respect of time and place of dispatch of data messages.

Article 10 sets out the deeming provisions contained in article 13 of the Model Law in regard to the allocation the risk in respect of delivery of electronic messages and sets out circumstances where the originator is deemed to have sent electronic messages.

Article 11 of the South Korean legislation provides for the individuality of electronic messages, where a data message sent to multiple addresses and deems each one to have been sent individually. This is not contained in the Model Law and may deal with the situation where a single electronic message is sent to multiple addressees.

Article 12 of the South Korean legislation invokes, verbatim, the acknowledgement of receipt procedures as set out in article 14 of the Model Law.

The reasons for the exclusion of a specific reference to articles 11 and 12 of the Model Law may lie in the existence of more detailed provisions set out in Chapter 3, providing security for electronic commerce. Article 16 provides for the government to designate an authorised certification authority to ensure the security and reliability of electronic commerce. The legislature's failure to refer to articles 11 and 12 of the Model Law may be well be intentional. The formation of electronic contracts under South Korean contract law may well be covered by the provisions of chapter 2 of the Bill. If this is so, it may be redundant to expressly provide for the conclusion of contracts where it the broad scope of effect given to signatures already provides this.

Chapter 4 - "Promotion of Electronic Commerce", of the legislation contains mainly statements of policy and statements of intent to foster electronic commerce. In themselves, *prima facie*, these do not appear to amount to statements of binding and enforceable law.

Part Three

Chapter Eleven - Malaysian Legislation

The Malaysian Digital Signature's Act of 1997

This legislation is based on the Malaysian Digital Signature's Bill of 1997 and was enacted in the same year. The Act deals primarily with the licensing of certification authorities and gives effect to digital signatures.[51]

Part One thereof contains the short title and definitions clauses.

Part Two thereof empowers the Minister to appoint a Controller of Certification Authorities and further empower such Controller to appoint a number of officers to issue licences to certification authorities for the purposes of monitoring and overseeing the activities of certification authorities.

In terms of section 4 of the Act, the licensing scheme is mandatory for the purpose of establishing a minimum regulatory system to provide a basic level of reliability in certification authority practice.

However, in terms of section 4, a digital signature is nevertheless given legal validity if verified by a certificate issued by an unlicensed certification authority or without verification by any certificate at all. Part Three expressly states that the licensing requirements under the Act shall not affect the effectiveness or enforceability of any signature. Section 4 provides that where such a digital signature is under dispute, the effect of not having a licence is that the liability limits specified in Chapter 8 of Part Four cannot be invoked by the certification authority to limit its liability.

In terms of section 60 of Part Four, contained in Chapter 8, a licensed Certification Authority shall, in issuing a certificate to a subscriber, specify and recommend a reliance limit in the certificate. The licensed Certification Authority may specify different limits, as it considers fit.

Liability limits are set for licensed Certification Authorities terms of section 61. Unless a licensed Certification Authority waives the application of the section and provided that the licensed Certification Authority has complied with the requirements of the Act, it shall not be

[51] <http://www.mycert.mimos.my/digital/sign13.html>

liable for loss caused by reliance on a false or forged digital signature in excess of the amount specified in the certificate as its recommended reliance limit.

In terms of the Act loss must be caused by reliance on a misrepresentation in the certificate and a certificate authority cannot be held liable for "punitive or exemplary damages" or for "damages for pain and suffering".

By specifying a recommended reliance limit in a certificate, the issuing certification authority and accepting subscriber recommend that a person rely on the certificate only to the extent that the total amount of risk does not exceed the recommended reliance limit.

Section 62 of Part Five provides that a digital signature shall be as legally binding as an affixed thumbprint or any mark and that any document may be signed by it.

Similarly sections 64 and 65 deem digitally signed documents to be written documents and original documents respectively.

From an analysis of the Act it would appear as if the Malaysian legislature has exercised its discretion in applying only Chapter 2 of the Model Law and has not gone to the extent of applying Chapter 3 dealing with contractual provisions. The legislation contains no provisions dealing with contract or with clauses 11 to 15 of the Model Law but gives effect to articles 5 to 10 of the Model Law.

It is submitted that the detailed provisions relating to the appointment of the Controller of Certification Authorities and the associated liability provisions do not remedy an essential defect in the Act, ie its failure to provide for the formation of contracts between parties under the domestic law.

To the extent that detailed provision is made for the validity and enforceability of digital signatures and digitally signed documents, the Act fails to consider the scope of applicability of such instruments and for what purposes they may be used. It is therefore submitted that the Act is more concerned with the executive control of certification authorities and less concerned with creating rules of certainty for electronic commerce in general or electronic contracts in particular.

Part Three

Chapter Twelve - United States of America Legislation

12.1 Federal Electronic Commerce Legislation

12.1.1 Article 2B

In the United States, article 2 of the Uniform Commercial Code (hereinafter referred to as the UCC), deals generally with sales. Section 2B has been amended on repeated occasions to allow for the application of traditional contracts or concepts to electronic contracting. The latest amendment dated March 1998 sets out guidelines for electronic contracting and reflects the Model Law. [52]

12.1.2 Background to Article 2B

In 1996, the National Conference of Commissioners on Uniform State Laws established a Drafting Committee on Electronic Communications in Contractual Transactions, later renamed the Drafting Committee on the Uniform Electronic Transactions Act (UETA), to consider the contracting issues raised by electronic commerce. [53]

In its drafts UETA relied directly on Chapter 3 of the Model Law, adopting, verbatim, its provisions on formation and validity, and effectiveness between the parties. In addition, the Model Law provisions on acknowledgement of receipt, time and place of dispatch and receipt or electronic messages were carried over into UETA.

However during the early 1990s, the Section of Science and Technology of the American Bar Association began to consider the legal impact of digital signatures involving the use of public key cryptography.

By 1996, the ABA had published a set of Digital Signature Guidelines, setting out policy issues that needed to be faced to implement a legal structure to support the use of digital signatures.[54]

The guidelines recommended the technology of public key cryptography with certificates to link the signer to a record, meeting the Model Law's test of appropriate reliability.

---

[52] <http://www.law.upenn.edu/library/ulc/ucc2/2b398.pdf>

[53] see above n 38

[54] The American Bar Association's Guidelines On Digital Signatures is available at <http://www.abanet.org/scitech/ec/isc/dsgfree/html>.

12.1.3 Rejection of the common law "mailbox" rule

Part 2 of the latest article 2B of the UCC deals with the formation and terms of the contract and expressly rejects the mailbox rule for electronic messages and adopts a time of receipt rule.[55]

12.1.4 Electronic Agents

An electronic agent is defined by article 2B as an automated system selected or used by a person for the purposes of achieving contract related effects such as offer and acceptance as well as performance of the contract itself, without a human being intervening.[56]

In terms of the legislation, a contract can exist where no human being reviews or reacts to the electronic message or information delivered. It allows for an automated system to send and react to messages without human intervention when parties choose these systems on the basis that direct human assent would inject an inefficient and error prone element in the modern electronic formation.

The electronic agent is regarded as an extension of the person utilising its actions, which are deemed to constitute those of the individual.

An electronic record, message or performance is attributable to a party if that party, its agent, or its electronic agent sent it.[57] This accords with article 13(2) of the Model Law which provides that a data message is attributable to a party if it was sent by an authorized agent of the party, or by an information system programmed by, or on behalf of, that party to operate automatically.

12.1.5 Acceptance that Varies the Terms of an Offer

Article 2 B allows for acceptance that varies terms of an offer. However when the varied acceptance conflicts with material term or amounts to a material modification of the offer contract formation is precluded based on such a purported acceptance.

---

[55] S 2B 120
[56] s 2B-102(a)(12)

12.2 State Level digital signature initiatives

Initiatives to implement a legal structure to support the use of digital signatures commenced at state level, rather than by the national law reform bodies. States competed to be at the centre of high-technology commerce, reducing incentives for co-operation. and the national law reform bodies considered the potential for signatures as well beyond the scope of their mandate. [58]

12.2.1 The 1995 Utah Digital Signature Act

Utah has a significant number of high-technology companies domiciled in the state, who lobbied for legislation and was the first to enact.[59] In 1996, the Digital Signature Act, which made a digital signature a complete substitute for a manual signature, provided that the digital signature was accompanied by a certificate showing the identity of the holder of the private key and that certificate was issued by a state-licensed certification authority.[60]

12.2.2 1995 Californian Legislation

California, the second influential United States state to adopt the Model Law, did not follow the Utah statute which aligned itself to public key cryptography and drafted a technology-neutral law, along the lines of the Model Law.[61] It provided that a digital signature would have the same legal effect as a manual signature under certain circumstances.

12.2.3 The 1998 Illinois Electronic Commerce Security Act

In Illinois, a large working group under the sponsorship of the Attorney General has prepared the Illinois Electronic Commerce Security Act. The Illinois Act speaks of a "secure electronic signature" rather than a digital signature. The Act does not deal with licensing or liability of certification authorities but imposes rules by setting criteria for trustworthiness of linkages relating to identity and record.[62] The bill implements a key concept of the Uncitral Model Law, article 7, ie that using a secure electronic signature creates a presumption that the signature is that of the person to whom it correlates.

The Act was introduced into the state legislature in February 1998, as House Bill 3180, and passed to the General Assembly on 20 May 1998 and was signed by the Governor on 14

---

[57] Under s 2B -211 (a) (1) of the UCC
[58] see above n 38
[59] The text of the Act is available at <http://www.le.state.ut.us/~code/TITLE46/46_03.htm
[60] See below in Chapter 13 for a more detailed analysis of specific digital signature legislation
[61] The text of the Act is available at <http://www.leginfo.ca.gov/pub/95-96/bill/asm/ab_2751-2800/ab_2755_bill_960925_chaptered.html>

August 1998. The chair of the group that produced the bill, Thomas Smedinghoff, joined the United States delegation to Uncitral in 1997.[63]

The then-current draft of the Illinois bill was presented in September 1997 to a meeting of experts assisting the Uncitral Secretariat in revising its initial draft model rules on digital signatures. It has influenced Uncitral 's working paper prepared by the Uncitral secretariat and considered by the Working Group in January 1998. [64]

Most other states have followed suit. Forty-nine States have either enacted or prepared digital signature legislation. However the provisions of the Model Law have not been adopted uniformly and the degree of validity and enforceability of a digital signature varies from State to State. For that reason only the main initiatives have been identified above and they are dealt with in more detail below .[65]

---

[62] <http://www.ag.state.il.us/resource/cecc/cecc2.htm>
[63]He is a partner in the law McBride Baker & Coles, based in Chicago and a respected author on Information technology Law < http://www.mbc.com/.>
[64] See below in Chapter 14 for a discussion of the Draft Rules
[65] For a more detailed analysis of the implementation of digital signatures in the United States <http://www.ilpf.org/digsig/survey.htm>

Part Four

Chapter Thirteen - Digital Signatures

While article 13 of the Model Law sets out the circumstances in which an electronic message is attributed to a person or company, these rules may be supplemented by electronic signature technology to provide a solution to problems of attributing electronic messages to a person or company.[66]

13.1 Asymmetric Cryptography

Digital signatures operate by using asymmetric cryptography in the form of a public key and a private key, known as a key pair. Messages are encrypted using a private key that is unique to the sender of the message. The message is unintelligible in its encrypted form, and cannot be altered after encryption. The message is then sent to the recipient who decrypts it using the matching public key. Unlike the private key, the public key component of a key pair is publicly available. A public key may also be used to encrypt a message, which would be decrypted by the corresponding private key.

13.2 The Distinction between an Electronic Signature and a Digital Signature

13.2.1 Electronic Signature"

An "electronic signature" has been defined as

> "any identifiers such as letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party to a transaction with an intent to authenticate a writing. ".[67]

A "writing" as defined by the Model Law, is deemed to be electronically signed if an electronic signature is logically associated with such writing.

13.2.2 Digital Signature

In contrast to an electronic signature, a "digital signature" has been defined as

> " an electronic identifier that utilizes an information security measure, most commonly cryptography, to ensure the integrity, authenticity, and non repudiation of the information to which it corresponds."[68]

13.3 Public Key Cryptography

Cryptography is based a field of applied mathematics in which digital information may be transformed into unintelligible code and subsequently translated back into its original form. In

---

[66] The New Zealand Law Commission report on Electronic Commerce at pg.130 see above n 21 for URL
[67] <http://www.ilpf.org/digsig/survey.htm> at pp. 4 to 5
[68] The definition of the American Bar Association, <http://www.abanet.org.scitech/ec/isc/dsg-tutorial.htm>;

public key cryptography, an algorithmic function is used to create two mathematically related or complementary "keys." One key is used to code the information while the other is used to decode it. Public key cryptography allows the confidential transmission of information in open networks where parties do not know one another in advance. [69]

13.4 Certification Authorities

Smedinghoff contends that public-private key pairs used to create digital signatures have no intrinsic association with anyone as they are nothing more than large numbers.[70] Therefore a third party trusted by both the sender and recipient must perform the tasks necessary to associate an identified person with the key pair used to create the digital signature. Such a trusted third party is called a Certification Authority, ascertains the identity of a person, called a "subscriber," and certifies that the public key of a public-private key pair used to create digital signatures belongs to that person"

The subscriber: would normally

13.4.1 generate a public/private key pair using software on his computer;

13.4.2. visit the Certification Authority and produce proof of identity; and

13.4.3. demonstrate that he holds the private key corresponding to the public key.

As Smedinghoff notes, certification processes vary from Certification Authority to Certification Authority as one Certification Authority may require a subscriber to appear in person before the Certification Authority as part of the second step of establishing the subscriber's identity while another Certification Authority may be willing to rely on a third party, such as a notary, to establish the subscriber's identity.

Once the Certification Authority has verified the association between an identified person and a public key, the Certification Authority then issues a certificate, a computer-based record that attests to the connection of a public key to an identified person or entity.

---

[69] idem supra 67

[70] Certification Authority Liability Analysis prepared for American Bankers Association; by: Thomas J. Smedinghoff, February 1998, <http://www.abaecom.com/docs/CALiability%20analysis.doc>

13.5 The Relationship between a Certificate and a Certification Authority

A certificate identifies the Certification Authority issuing it and the person (called a subscriber) identified with the public key. The certificate also contains the subscriber's public key and other information, such as an expiration date for the public key. To provide assurance as to the authenticity and integrity of the certificate, the Certification Authority attaches its own digital signature to the certificate.

The Certification Authority notifies the subscriber that the certificate has been issued so as to give the subscriber an opportunity to review the contents of the certificate before it is made public. If the subscriber finds that the certificate is accurate, the subscriber may publish the certificate, or direct the Certification Authority to do so, making it available to third parties who may wish to communicate with the subscriber. A certificate is published by being recorded in one or more repositories or circulated by any other means so as to make it accessible to all intended correspondents. A repository is an electronic database of certificates which are generally available online.

13.6 Use of the Key Pair

In an open network context, such as the Internet, public key encryption depends on the public and private use of these complementary algorithmic keys. The public key is associated with a particular party and is made readily available in a repository. The private key however must remain secret in order for the process to be secure, for while the public key of a particular party is known to the public, only the private key can be used to decrypt a message. In addition, the public key itself is used to encrypt a message or data to be sent to the person associated with the key. The recipient of the encrypted message uses his or her private key to decrypt the information.

The private key encryption programme code cannot be replicated or broken from the public key so that messages encrypted by private key A can only be decrypted by public key A, and public key A cannot be used to decrypt any other message.[71]

13.7 The Utah Digital Signature Act (1995)

This Act was the first Act of its kind and defines a digital signature as

> "a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key

---

[71] The New Zealand Law Commission report on Electronic Commerce at pg.131 see above n 21 for URL

can accurately determine whether:
(a) the transformation was created using the private key that corresponds to the signer's public key; and
(b) the message has been altered since the transformation was made."[72]

The Utah Act allows only digital signature technology using public key cryptography. Alternative electronic signature technology is not covered by the Utah Act.

The Utah Department of Commerce Division of Corporations and Commercial Code is a certification authority responsible for issuing, suspending and revoking private keys. .[73] The division may also license other certification authorities providing they meet security criteria.[74] The Act provides that duly authorized digital signatures may be used to meet statutory requirements of signed writing.[75] and that messages which bear digital signatures are as valid, enforceable and effective as if they were written on paper.[76]

Section 46-3-402 provides:

> "Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances. If the recipient determines not to rely on a digital signature pursuant to this section, the recipient shall promptly notify the signer of its determination not to rely on the digital signature."

13.8 California Government Code (1995)

The California Government Code was amended in 1995 to allow the use of electronic signatures in communications with "public entities". Section 16.5 provides:

> "16.5 (a) In any written communication with a public entity, as defined in Section 811.2, in which a signature is required or used, any party to the communication may affix a signature by use of a digital signature that complies with the requirements of this section. The use of a digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:
> (1) It is unique to the person using it.
> (2) It is capable of verification.
> (3) It is under the sole control of the person using it.
> (4) It is linked to data in such a manner that if the data are changed; the digital signature is invalidated.
> (5) It conforms to regulations adopted by the Secretary of State."

---

[72] Utah Code s 46-3-103(10))
[73] Utah Code s 46-3-104 (1)
[74] Utah Code s 46-3-201
[75] Utah Code s 46-3-401
[76] Utah Code s 46-3-403

The section is limited in that it only provides that electronic signatures are legally effective as signatures in transactions with public entities.

A digital signature is defined as

> "an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature."

Only "acceptable technologies" be used.[77] The approach of the Californian State Legislature contrasts with the approach of the Utah Act which only allows digital signature technology using public key cryptography.

Pursuant to s22003 of the draft regulations to the Act either digital signature or signature dynamics technologies are currently approved. In terms of s22004 or new technologies may be added to the list.

The draft regulations provide for licensing of certification authorities for the use of digital signatures, but does not seek to allocate commercial risks for users, again in contrast to the Utah Act.

The Digital Signature Regulations approved by California Secretary of State 12 June 1998 do not alter the established position substantially.

13.9 Digital Signature Act 1997 (Federal Republic of Germany)[78]

This Act was passed as Article 3 of the Information and Communication Services Act (Informations-und Kommunikationsdienste-Gesetz) on 1 August 1997.

It includes subordinate legislation in the form of the Digital Signature Ordinance (The Signatureverordnung, decreed under s 16 of the Digital Signature Act and entered into force on 1 November 1997).

Section 1(1) of the German statute provides that the purpose of the Act is to establish general conditions under which digital signatures are deemed secure and to establish

---

[77] California Government Code Section 16.5(a)(5), (18 November 1997).

[78] An English copy of Article 3 of the Informations- und Kommunikationsdienste-Gesetz - IuKDG) of August 1 1997 is available at <http://www.iid.de/rahmen/iukdgebt.html#a3>

procedures by which forgeries of signatures or manipulation of signed data can be reliably ascertained.

Like the Utah Act, it is technologically specific, defining a digital signature as a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority.[79]

The German Act and its subordinate legislation, the Digital Signature Ordinance, provides a code for the establishment and regulation of certification authorities. Under section 3 of the Act, certification authorities must be licensed by the state.

Section 15 provides for recognition of digital signatures issued in another member state of the European Union or contracting state to the Treaty on the European Economic Area, provided the signature is subject to comparable levels of security.

[79] (s 2(1))

Part Four

Chapter Fourteen - Uncitral Draft Articles On Electronic Signatures

At the 34th session of the working group on electronic commerce, convened under the auspices of Uncitral, held in Vienna from the 8th to the 19th February 1999, 17 draft articles on electronic signatures were tabled before the members of the working group.[80]

The commission elected to maintain a consistent approach to the media neutrality expressed in the Model Law and therefore elected to provide a broad definition of electronic signatures in compliance with article 7 of the Model Law. For that reason the working group avoided aligning itself with the dominant role played by public key cryptography.[81]

The working group considered that one of the main purposes of the draft uniform rules was to establish a minimum set of standards to be met by certification authorities, in particular where cross border certification was sought, so maintaining the international perspective rationale adopted in the Model Law.

14.1 Definitions

The definition of "electronic signature" is set out widely in a manner consistent with the provisions of the Model Law. The definitions clause refers to an "enhanced electronic signature" which is defined as

> "an electronic signature which can be verified through the application of a security procedure or combination of security procedures that ensures that such electronic signature":
>
> (i) is unique to the signature holder;
> (ii) can be used to identify objectively the signature holder in relation to the data message;
> (iii) was created and affixed to the data message by the signature holder, or using a means under the sole control of the signature holder."

The text defines a Certification Authority as “an information certifier”

> "...a person or entity which in the course of business engages in providing identification services which are used to support the use of enhanced electronic signatures."

---

[80] <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-80.htm>

[81] Another method of user authentication over a WAN is by the use of server-based software used in conjunction with physical, hand-held tokens which hold a solid-state chip, generating a "once-off" algorithms which to identify and validate the user for each session

14.2 Draft Article B

This article of the text confirms article 7 of the Model Law and restates the principle of article 7 that an electronic signature can satisfy a requirement of law for a signature provided that meets certain conditions.

14.3 Draft Article C

This confirms article 8 of the Model Law to provide that an electronic signature can satisfy a requirement of law for an original, provided that it meets certain conditions. This article allows the enacting state to designate an organ or authority to have the power to determine what specific technologies qualify as an enhanced electronic signature within the definition of the draft.

14.4 Draft Article D

This article confirms that any determinations by the enacting state should be consistent with recognised international standards and thereby recognises that an enhanced electronic signature will not prejudice third parties.

14.5 Draft Article E

This article reaffirms the importance of party autonomy consistent with the approach in article 4 of the Model Law and reaffirms the bilateral freedom of contract which parties may elect to govern the relations between them.

> "A signature holder and any person who may rely on the electronic signature of the signature holder may determine that as between themselves the electronic signature is to be treated as an enhanced electronic signature."

14.6 Draft article F

This article sets out the obligations of the signature holder and establishes minimum standards that a signature holder is obliged to observe in holding and using a signature. These would include notification where the signature is compromised in its dealings with certificate authorities and relying parties.

14.7 Draft Article G

This article develops the principle contained in article 13.3 of the Model Law by allowing a party to rely on an enhanced electronics signature only if it takes reasonable steps to determine that the enhanced electronic signature is valid and has not been compromised or revoked. The reasonable steps envisaged in the text include:

14.7.1 confirming information made available by a certification authority as to the validity of the signature that is it certified;

14.7.2 verifying a signature using a procedure agreed with the signature holder.

14.8 Draft article H

14.8.1 Draft Article H(1) sets out minimum obligations of an information certifier

14.8.2 Draft article H(2) invokes a sanction for the failure to meet these obligations by creating liability for the information certifier for the consequences of failure to comply with a list of obligations contained in the draft article.

14.8.3 The text expressly avoids setting out the nature of the sanction and leaves this to the domestic state.

14.8.4 The obligations envisaged in terms of sub-article (1) are to:

"a) act in accordance with the representations it makes with respect to its practices;

(b) take reasonable steps to determine accurately the identity of the signature holder and any other facts or information that the information certifier certifies;

(c) provide reasonably accessible means which enable a relying party to ascertain:

(i) the identify of the information certifier;

(ii) the method used to identify the signature holder;

(iii) any limitations on the purposes for which the signature may be used; and

(iv) whether the signature is valid and has not been compromised.

(d) Provide a means for signature holders to give notice that an enhanced electronic signature has been compromised.

(e) Ensure that all material representations or statements the information certifier makes are accurate and complete to the best of it's knowledge and belief;

(f) Utilize trustworthy systems and procedures in performing its services."

Part Five

Chapter Fifteen - Findings

15.1 Decided Cases

Depending on how one categorises an Internet contract, the line of cases indicate that while such a contract concluded over the Internet may be valid, its enforceability may well be in question. While the writer contends that the current legislative provisions permit the party relying on such a contract a degree of latitude, much depends on how such a case is presented before a court of Law and how the court interprets the applicable statute.

This is unlikely to create confidence in Internet commerce. Legislation would provide the certainty required for such confidence.

15.2 The Model Law

On the whole, the Model Law has been implemented in most jurisdictions studied in this dissertation. While certain jurisdictions such as Australia gave the impression that they considered that the legislation could impose on aspects of their common law of contract; certain other jurisdictions such as Singapore felt that the Model Law did not go far enough.

However most jurisdictions invoked the provisions of Chapter 2 of the Model Law. Australia, Malaysia and South Korea had reservations about certain parts of Chapter 3, while Singapore supplemented Chapter 3 with additional security related provisions. Countries such as Germany and Malaysia appeared to be more concerned about regulation and less concerned about promoting electronic commerce. Yet one could contend that they provide a secure environment to foster electronic commerce.

Singapore has elected not to affect its Law relating to deeds for the transfer of immovable property, mortgage bonds, trust deeds, negotiable instruments, wills or codicils powers of attorney. This reflects prudent alignment with their domestic law to cause minimal disruption.

15.3 The- Uncitral Draft Articles on Electronic Signatures

The working group members of Uncitral have not stopped their work. They have incorporated the domestic digital signature initiatives taken by the various member states in the Uncitral Draft Articles on Electronic Signatures. The articles are the result of co-operation between the working group members and the representatives of the member states. They reflect both the momentum gained by the implementation of the Model Law as well as the

input of the individual member states, based on their experience of national digital signature legislation.

It is submitted that this "second wave" represents collective recognition of the need for more certainty than that currently provided by the Model Law with specific regard to:

15.3.1. The role, duties and liabilities of certificate authorities.

15.3.2 The positive role that enhanced digital signatures can provide to both domestic and international commercial interests who seek to implement electronic commerce.

15.4 Authentication

Proponents of Internet commerce claim that the primary advantage of Internet commerce is its ability to transcend the limitations of territoriality and geography. This may be correct, but the main issue which the Uncitral working groups as well as domestic legislatures attempt to address by their efforts is as a direct result of the nature of "cyberspace".

15.4.1 With whom am I transacting?

The medium is impersonal and anonymous. Parties do not know each other. This effects a basic contractual foundation, namely the identity of the parties. In a more conventional commercial setting, the identity of the parties is seldom an issue as their identities are readily established. Parties communicate, negotiate and make counter offers with each other. The converse appears to be true of the Internet. The terms and conditions on a website are seldom open for negotiation. An offeree either accepts them or not. Having agreed on the terms and conditions of contract, the parties then go about identifying one another.

15.4.2 The Court's Demonstrated Flexibility in Dealing with Authentication

Parties conclude agreements for the sale of immovable property on the basis that both the seller and the buyer have a mutual interest in the fulfilment of its terms and conditions. The sale of an immovable property is an everyday transaction which does not usually involve a dispute over the contract. Where it does, the parties must look to the courts.

South African courts have often given effect to an inferred intention of the parties by acknowledging that where authentication is required to meet the requirements of statute, the information representing authentication can take the format of a telegram or phonograms.

The courts have recognised that a party's intention stands behind form. While this principle may be extended to telefaxes at some future date, as similar provisions apply, until such future date, interested observers must refer to general principles.

Our courts have attempted to give effect to contract by determining the parties' intentions regardless of the mode of communication used, where the ambit of the contract affords such interpretation and provided that, by giving effect to the parties' intentions, they do not condone statute contravention.

Yet can the South African system of precedence be expected to deal with the novelty of electronic commerce and are commercial interests willing to submit themselves to our system of precedence and the accompanying risk?

While the answer to the first part may be positive, the answer to the second is more likely to be negative. It may relate more to the lack of confidence of commercial interests, caused by the uncertainty of the Internet itself than by the general principles of South African Contract Law.

Therefore, where authentication in a medium of communication is a source of uncertainty, the source of that uncertainty should be addressed, not the consequences of that uncertainty. A simple way to achieve this would be avoid the medium and so its range of consequences by not contracting on the Internet.

It is submitted that acceptance of the feasibility of digital certificates "underwritten" by certification authorities addresses the issue of authentication at its root and encourages freedom of contract.

However, the pragmatic acceptance of technological innovation invariably has further implications for the Law. The German, Utah, Malaysian and Singapore legislation, as well as the Uncitral Draft Articles on Electronic Signatures manifest these implications by their understanding and expression of the need to regulate and control certification authorities.

Part Five

Chapter Sixteen - Recommendations

This dissertation has attempted to review how the law has responded to a specific technology or a suite of technologies. While the Internet appears to be a novel innovation, at some point in our history the telegram and telephone must have appeared equally novel. The Law does not exist in isolation and it does eventually respond to change.

It cannot be said with any certainty that an Internet contract is either valid, binding or enforceable in South African law. This area remains a *lacuna* which requires legislation, despite the apparent willingness of our courts to accept the effect of innovative modes of communication technology on Contract Law, when such cases appear as disputes before them.

However, if one accepts the importance of the role of electronic commerce in the future, any proposed legislation should be carefully planned and the full range of available options must be considered. It is submitted that the South African legislature can learn from the experience of other countries in this regard.

If one accepts the reality of an increasingly important role of electronic commerce in a global economy and the implications this holds for a developing and geographically isolated country such as South Africa, it is submitted that merely invoking the provisions of the Model Law as they currently stand would provide prompt relief, requiring further attention at a future date.

Inasmuch as the Australian Attorney-General has recommended to Parliament not to invoke any specific regulations for digital signatures or for the regulation of certification authorities, the issues relating to digital signatures and certification authorities are unlikely to wane. Therefore additional legislation may be required to supplement the current Australian Bill.

If South Africa is to compete with First World nations in a global economy then it may look to the approach of a small, geographically isolated country like Singapore which has few natural resources. Singapore has identified the potential that electronic commerce holds and has mapped its Law to its economic aspiration of becoming a recognised hub of electronic commerce activity.

At the same time it must be stated that the Model Law is well drafted, lucid on the issues relating to contracting using modes of telecommunication and could be easily be enacted as it stands, without a single amendment.

However inasmuch as Uncitral itself has identified the need to supplement its own Model Law, legislatures intending to invoke the provisions of the Model Law should read caution into the very basis for the Uncitral Draft Articles On Electronic Signatures.

Are the issues so pressing that legislation needs to be enacted as a matter of extreme urgency? If so, the current lacuna in South African law could well be remedied to a large extent by simply invoking the provisions of the Model Law. In order to cause minimal disruption to existing paper based systems, such legislation should not modify our law relating to deeds for the transfer of immovable property, mortgage bonds, trust deeds, negotiable instruments, wills or codicils and notarised contracts as set out in Chapter Five above.

Or should the matter rather be referred to the South African Law Commission for the formation of a Working Group to consider appropriate alternatives? Legislation has a long gestation period. Once the process starts, it is difficult to alter course. If a cautious approach would be more advisable, it may be more prudent for the South African legislature to table detailed legislation which deals with the full range of issues including an approach to digital signatures and certification authorities, after consultation with all stakeholders.

Is this not ultimately a question of executive policy?

The former approach would involve less disruption to the common law provisions while the latter would arguably provide more economic leverage to compete in the information age.

Appendix A

Table Of Cases

Appendix B

Table of Articles or Publications Referred to

Appendix C

Table Of Statutes

Domestic

Act	Number	Year	Section(s)	PageNumber(s)
Deeds Registries Act	47	1937	50(1), 87, 61	24
Wills Act	7	1953	52	24
General Law Amendment Act	50	1956	6	24
The Bills of Exchange Act	34	1964	52, 87, 95	24
Stamp Duties Act	77	1968	12	25
Formalities in respect of	-	-		24
Leases of Land Act	18	1969	1	24
Alienation of Land Act	68	1981	2(1)	24
Credit Agreements Act	75	1980	5 (i), 5(2)	24
Computer Evidence Act	57	1983	1 to 7	29
Law of Evidence Amendment Act	45	1988	3	32
Trust Property Control Act	57	1988	1	24
Amendment Act	5	1992	1	29
Telecommunications Act		1996	5, 40	12

International

	Year	PageNumber(s)
The Vienna Sales Convention	1980	37
The Utah Digital Signature Act	1995	59, 63
California Government Code (1995) Legislation	1995	59, 64
The UNCITRAL Model Law on Electronic Commerce	1996	37, 39 -48
The Malaysian Digital Signature's Act	1997	55
Information and Communication Services Act (Federal Republic of Germany)	1997	65
The Singapore Electronic Transactions Act	1998	51
Article 2B of the Uniform Commercial Code	1998	38, 57
The 1998 Illinois Electronic Commerce Security Act	1998	59
The South Korean Basic Law on Electronic Commerce	1999	53
Australian Electronic Transactions Bill	1999	50

Appendix D

URL'S of Internet Resources Referred To

Bibliography

Computer and Information Law Digest, James A Douglas, Laurel Binder Arain, Warren Gorham & Lamont 1994.

The Internet Navigator, 2nd edition Paul Gilster, John Wiley & Sons Inc. 1994.

The South African Law of Evidence; LH Hoffmann, D T Zeffert, 4th edition Butterworths 1989

The Principle of the Law of Contract; A J Kerr 4th edition Butterworths 1989

The Law of Agency; A J Kerr 3rd edition Butterworths 1991

Management Information Systems; K C Laudon, J P Laudon Prentice Hall International Inc. 1996

Internetworking with Microsoft TCP/IP and Microsoft Windows NT 4.0 Workbook. 1997. Microsoft Corporation

Computer Law, 3rd edition Chris Reid ed. Blackstone Press Ltd. 1990.

Computer Law. Law and Technology Library; M D Scott.(Ed) Wiley Law Publications, John Wiley & Son. 1987.

Business Transaction Law, Robert Sharrock, 4th edition . Juta and Co. 1996

Computer Law, Colin Tapper 4th edition. Longman Group 1989.

Computers & The Law; D P Van Der Merwe Juta & Co Ltd 1986